Elliptic Curve Public Key Cryptosystem

Alfred Menezes 저
한국과학기술원 전산학과 김 광조 역
본 자료는 2010년 봄학기에 개설된 고급정보보호의 학습용임

2010년 5월 일

목 차

제 1 장

타원곡선 암호시스템의 개요

타원 곡선은 개수 기하학과 정수론 등에서 집중적으로 연구되어 왔으며, 이 주제에 관하여는 상당한 책이 발간되어 있다. 최근에는 소인수 분해[80, 105, 106, 143]와 소수 판정법[7,48,125]에 유용한 알고리즘을 설계하는 데 사용되어 왔다. 암호학의 연구에는 타원 곡선은 공개키 암호 시스템[67,100], 의사 난수 발생기[62,63], 일방향 치환[64]의 구성에 활용되고 있다. 다른 활용 분야로는 부호이론 중 양호한 오류 정정 부호[36,46,147]을 구하는 데 이용된다.

타원 곡선 암호 시스템은 기존의 공개키 암호 시스템에 비해 짧은 키의 길이로 동등한 안전성을 잠재적으로 제공한다. 짧은 키 길의, 적은 대역 폭, 적은 메모리 등은 스마트 카드 등에 응용하는 데는 가장 중요한 요소로 작용한다. 이 책은 타원 곡선을 이용한 효율적인 안전한 공개키 암호 시스템을 구현하는 가능성을 다방면으로 연구한다.

이 책의 내용은 자체적으로 충분한 내용을 포함하였다고 생각하나, 초심자의 경우에는 Koblitz의 책[68] 중 6장을 우선 읽는 것이 유용할 것이다.

2장에서는 유한 체 상에서 타원 곡선에 관한 적절한 이론을 요약한다. 3장에는 표수 2의 유한체 상에서 다양한 타원 곡선의 수를 세어보고 정리한다. 이 장의 결과는 암호 시스템을 구현하는 데 적절한 곡선을 선택하는 데 유용할 것이다.

4장에서는 이산 대수 문제에 관한 알려진 알고리즘을 간단히 기술한다. 특이 타원 곡선을 포함하여 어떤 군에서 대수 문제는 유한체 상의 대수 문제로 축소되는 가를 제시한다. 5장에서는 타원 곡선의 대수 문제를 유한체 상 대수 문제로 축소하는 것을 다룬다. 이 축소는 타원 곡선의 특별한 부류, 즉 초특이 타원 곡선에 유용하다. 이 결과로 암호 시스템을 설계할 때 타원 곡선과 기반

체를 선택하는 데 주의하여야 한다.

6장에서는 타원 곡선 암호 시스템의 효율적인 구현에 대하여 여러가지 문제를 고려한다. 이런 시스템은 하드웨어나 소프트웨어에 모두 실용적이고 적합한 것을 제시한다.

곡선의 선택은 이산 대수 문제에 대한 알려진 공격법에 강하도록 하는 대단히 중요한 작업이다. 7 장에서는 표수 2의 유한체 상에서 타원 곡선의 점을 계수하는 Schoof 알고리즘을 향상시키는 알고리즘을 제시한다.

이 자료는 한국 정보 통신 대학원 대학교의 1999년 2학기 암호와 정보보안 특강의 수강생에게 타원 곡선 암호 시스템의 연구와 응용에 보탬이 되고자 Menezes의 책 중 공개키 암호 시스템에 관한 1장의 내용을 생략하고 모든 내용을 번역하였다. 이 책자를 통하여 타원 곡선 암호 시스템 연구에 국내 연구자들에 도움이 되기를 희망하며, 아직 저자와 출판사와 저작권에 관련 된 사항이 협의되지 아니하여 정식 출간을 추후에 검토할 예정이다.

제 2 장

타원 곡선의 소개

이 장에서는 타원 곡선에 대한 기본 개념을 소개하고 널리 이용될 수 있는 여러 가지 결과를 기술한다. 모든 것을 전부 소개는 못하고 Koblitz의 책[68]의 6장에 내용을 확장한다. 별도로 언급되지 아니하였으면, 본 결과의 증명은 J. Silvermann의 책[140]에서 찾을 수 있다. 타원 곡선에 대한 기본 개념을 이해하기 위하여는 Charlap과 Robbins의 책[26]과 최근의 책으로 Silverman과 Tate 책[141]을 권고한다.

제 1 절 정의

F_q는 q개의 요소를 가진 유한 체로 표기하고 q는 소수의 멱승이라고 하자. 만일 K가 체라면 $\overline{K}$는 체의 대수학적 폐 (algebraic closure) 라고 하자. (만일 $K = F_q$ 이면, $\overline{K} = \cup_{m \geq 1} F_{q^m}$ 이다.) K 상의 투영 공간 (projective plane) $P^2(K)$는 $K^3 \backslash \{(0,0,0)\}$ 상의 작용하는 관계 $\sim$ 의 등가 관계의 집합으로 $u \in K^*$가 존재하여 $x_1 = ux_2, y_1 = uy_2, z_1 = uz_2$가 되는 $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ 이다. 이런 (x, y, z)를 포함하는 등가 관계를 $(x : y : z)$로 표기한다. Weierstrass 방정식은 다음과 같은 형태로 차수가 3차인 homogeneous 방정식이다 .

$$Y^2Z + a_1XYZ + a_3YZ^3 \;=\; X^3 + a_2X^2Z + a_4XZ^2 + a_4XZ^2 + a_6Z^3$$

여기서 $a_1, a_2, a_3, a_4, a_5, a_6$는 $\overline{K}$의 원소이다.

만일 투영 공간 상의 모든 점 $P = (X : Y : Z) \in P^2(\overline{K})$

$$F(X,Y,Z) \;=\; Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0$$

을 만족하고 3개의 편미분 $\frac{\delta F}{\delta X}, \frac{\delta F}{\delta Y}, \frac{\delta F}{\delta Z}$ 중 점 P에서 적어도 한 개는 0이 아닌 경우 Weierstrass 방정식은 smooth 또는 non-singular 라고 한다. 그리고 어떤 점 P에서 모든 편 미분 값이 0이 되면 P는 singular라고 하고 Weierstrass 방정식은 singular라고 부른다.

타원 곡선 E은 (genus 1인 대수 곡선) smooth Weierstrass 방정식의 $P^2(\overline{K})$상에 모든 해의 집합을 의미한다. Z 좌표 값이 0이 되는 E 상에 점이 한 개가 존재한다. 즉, (0:1:0)이며 이 점을 무한 원점 (point at infinity) 이라고 하고 $\mathcal{O}$로 표기한다.

편의 상 타원 곡선을 위한 Weierstrass 방정식은 아핀 좌표 x = X/Z, y=Y/Z를 이용하면

$$y^2 + a_1xy + a_3y \;=\; x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

이 된다.

타원 곡선 E는 무한대 점 $\mathcal{O}$를 포함하고, 아핀 평면 $A^2(\overline{K}) = \overline{K} \times \overline{K}$에서 식(2.1)의 모든 해의 집합이다. 만일 $a_1, a_2, a_3, a_4, a_5, a_6$가 K의 원소가 되면 E는 K 상에서 정의된다 (defined over K)라고 하고 E/K라고 표기한다. 만일 E가 K 상에서 정의되면 E의 유리수 점을 E(K)라고 표기하고 $\mathcal{O}$ 점을 표함하여 K 상의 2개 좌표 값들의 집합이 된다. 식(2.1)를 간단히 E라고 표기한다.

투영 다양체 (projective varieties)로서 2개의 타원 곡선이 동형이면 (isomorphic) 2개의 타원 곡선은 동형이라고 한다. 간단히 하면, 체 K 상에 정의되는 2개의 투영 다양체 V_1, V_2는 만일 사상 $\phi : V_1 \to V_2, \psi : V_2 \to V_1$ (ϕ, ψ는 K상에서 정의됨)이 있어 $\psi \circ \phi$ 와 $\phi \circ \psi$가 각각 V_1과 V_2에 identity map이 되면 K 상에서 동형이라고 한다. 다음의 결과는 타원 곡선의 동형이라는 개념과 곡선을 정의한 Weierstrass 방정식의 계수와의 관계를 나타낸다.

정리 2.1 *다음의 방정식으로 주어지는 2개의 타원 곡선 E_1/K, E_2/K가*

$$\begin{aligned} E_1 : y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6 \\ E_2 : y^2 + \overline{a}_1xy + \overline{a}_3y &= x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6 \end{aligned}$$

$E_1/K \cong E_2/K$로 표시하는 K 상에 동형이 되는 필요 충분 조건은 K 상에 원소로 $u(\neq 0), r, s, t$가 존재하여, 변수의 변환

$$(x, y) \;\to\; (u^2x + r, u^3y + u^2sx + t) \tag{2.2}$$

가 E_1을 E_2로 변환할 때이다. 동형 사상의 관계는 등가 관계 (equivalent relation)이다.

식(2.2)의 변수 변환을 허용하는 변수 변환 (admissible change of variables)라고 부른다. 만일 K 상에 $E_1 \cong E_2$ 이고 식(2.2)가 방정식 E_1을 E_2로 변환한다면, 변수 변환

$$(x, y) \;\; \rightarrow \;\; (u^{-2}(x-r), u^{-3}(y-sx-t+rs)) \tag{2.3}$$

은 방정식 E_2를 E_1으로 변환하는 것으로 식 (2.3)는 허용하는 변수 변환이 된다. 또한,

$$\phi : (x, y) \;\; \rightarrow \;\; (u^{-2}(x-r), u^{-3}(y-sx-t+rs)) \tag{2.4}$$

는 E_1의 점을 E_2의 점으로 사상하고

$$\psi : (x, y) \rightarrow (u^2x + r, u^3y + u^2sx + t) \tag{2.5}$$

는 E_2의 점을 E_1의 점으로 사상한다.

그러면 K 상에서 $E_1 \cong E_2$이면 식(2.2)의 변수 변환은 방정식 E_1을 방정식E_2로 변환한다. 이 것은 다음의 방정식의 형태를 갖는다.

$$\begin{aligned}
u\overline{a}_1 &= a_1 + 2s \\
u^2\overline{a}_2 &= a_2 - sa_1 + 3r - s^2 \\
u^3\overline{a}_3 &= a_3 + ra_1 + 2t \\
u^4\overline{a}_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\
u^6\overline{a}_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1
\end{aligned} \tag{2.6}$$

다음의 정리는 정리(2.1) 과 같다.

정리 2.2 *K 상에 2개의 타원 곡선 E_1/K 와 E_2/K이 동형이 될 필요 충분 조건은 K 상의 원소 $u(\neq 0), r, s, t$ 가 식(2.6)를 만족 할 때이다.*

제 2 절 군의 법칙

타원 곡선 상의 점들은 어떤 덧셈에 대하여 아벨 군을 형성하는 것은 잘 알려져 있다. E를 식(2.1)으로 주어지는 타원 곡선이라고 하자. 덧셈 규칙은 다음과 같다. 모든 $P, Q \in E$에 대하여

(i) $\mathcal{O}+P=P, P+\mathcal{O}=\mathcal{P}$. ($\mathcal{O}$는 항등원이 된다.)

(ii) $-\mathcal{O}=\mathcal{O}$

(iii) 만일 $P=(x_1,y_1)\neq\mathcal{O}$ 이면, $-P=(x_1,-y_1-a_1x-a_3)$이다. P와 $-P$는 E상에 x 좌표가 x_1 이 되는 유일한 점임을 주의한다.

(iv) 만일 $Q=-P$이면, $P+Q=\mathcal{O}$

(v) 만일 $P\neq\mathcal{O}, Q\neq\mathcal{O}, Q\neq -P$ 이면 R은 $P\neq Q$이면 선분 $\overline{PQ}$과 또는 $P=Q$이면 P 상에서 접선($P=(a,b)$에서 곡선 $f(x,y)=0$의 접선은 $\frac{\delta f}{\delta x}(P)(x-a)+\frac{\delta f}{\delta y}(P)(y-b)=0$ 이 되는 선이다.) 이 만나는 제 3의 교점을 R이라 하면 $P+Q=-R$이 된다.

정리 2.3 *(E,+)는 항등원 $\mathcal{O}$을 가진 덧셈군이 된다. 만일 E가 K 상에 정의되면 E(K)는 E의 부분 군이다.*

정리(2.3)을 증명하는 어려움은 덧셈 규칙에서 결합 법칙을 증명하는 것이다. 2 가지 증명법으로 [24]에 기하학적 방법이 있고 [26]에는 divisor 이론을 이용한 대수학적 방법이 있다.

식(2.4)에서 정의한 ϕ는 $E_1(K)$와 $E_2(K)$간의 군 동형이다. 따라서 만일 $E_1/K\cong E_2/K$ 이면 $E_1(K)$와 $E_2(K)$는 아벨 군으로 동형이 된다. 역은 일반적으로 사실이 아니다.

경우(v)에서의 P와 Q의 좌표 값으로 $P+Q$의 계산식을 구하는 것은 쉽다. $P=(x_1,y_1)$, $Q=(x_2,y_2)$, $P+Q=(x_3,y_3)$라 하자. 만일 $P\neq Q$이면 l은 P와 Q를 지나는 선분 또는 $P=Q$이면 P상에서의 접선이라고 하자. l의 기울기는

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}, & \text{if } P\neq Q,\\[2ex] \dfrac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}, & \text{if } P=Q.\end{cases}$$

만일 $\beta=y_1-\lambda x_1$이면 l을 정의하는 방정식은 $y=\lambda x+\beta$가 된다. l과 곡선과 만나는 제3의 교점을 구하기 위하여는 $y=\lambda x+\beta$를 식(2.1)에 대입하면

$$x^3+a_2x^2+a_4x+a_6-(\lambda x+\beta)^2-a_1x(\lambda x+\beta)-a_3(\lambda x+\beta) \;=\; 0 \quad (2.7)$$

그러면 식(2.7)의 근을 x_1, x_2, x_3라고 하면 인수 분해가 되어

$$(x - x_1)(x - x_2)(x - x_3) = 0 \tag{2.8}$$

식(2.7)와 식(2.8)에서 x^2의 계수를 비교하면

$$-(x_1 + x_2 + x_3) = a_2 - \lambda^2 - a_1\lambda.$$

따라서

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

이고

$$y_3 = -(\lambda + a_1)x_3 - \beta - a_3$$

가 된다.

만일 $P, Q \in E(K)$이면 $P + Q$의 계산은 체 K 상에서 간단한 산술 연산에 의하여 되며 K가 유한체이라면 $P + Q$는 (결정적) 다항식 시간에 가능하다.

제 3 절 판별식과 j-불변량

E를 식(2.1)과 같이 주어 졌다면 다음을 정의한다.

$$\begin{aligned}
d_2 &= a_1^2 + 4a_2 \\
d_4 &= 2a_4 + a_1a_3 \\
d_6 &= a_3^2 + 4a_6 \\
d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= d_2^2 - 24d_4 \\
\Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \qquad (2.9) \\
j(E) &= c_4^3/\Delta \qquad (2.10)
\end{aligned}$$

Δ 값을 Weierstrass 방정식의 판별식이라고 하고 $j(E)$는 만일 $\Delta \neq 0$이면 j-불변량이라고 한다. 다음의 정리는 위의 2 가지 값의 의미를 정의한다.

정리 2.4 *E는 타원 곡선이 되는 필요 충분 조건은 $\Delta \neq 0$인 Weierstrass 방정식이 non-singular 이어야 한다.*

정리 2.5 *만일 E_1/K 와 E_2/K 가 K상에 동형이 되면, $j(E_1) = j(E_2)$이다. 만일, K가 대수적으로 닫혀있는 체라 하면 역도 성립한다.*

제 4 절 표수가 2나 3이 아닌 K상의 곡선

만일 타원 곡선이 표수 (characteristic)이 2나 3이 아닌 체 K 상에 정의된다면, Weierstrass 방정식은 상당히 간단히 된다. E/K를 식 (2.1)에 의하여 주어지는 타원 곡선이라고하면 만일 $char(K) \neq 2$이면 허용하는 변수 변환으로

$$(x, y) \rightarrow (x, y - \frac{a_1}{2}x - \frac{a_3}{2})$$

이 E/K를 다음과 같이 변환한다.

$$E'/K : y^2 = x^3 + b_2x^2 + b_4x + b_6$$

K 상에서 $E \cong E'$임을 주의하라.

만일 $char(K) \neq 2, 3$이면 허용하는 변수 변환으로

$$(x, y) \rightarrow (\frac{x - 3b_2}{36}, \frac{y}{216})$$

이 E'을 다음과 같이 변환한다.

$$E''/K : y^2 = x^3 + ax + b$$

역시 K 상에 $E' \cong E''$ 이므로 K상에 $E \cong E''$가 된다.

만일 $char(K) \neq 2, 3$이면 E/K의 형태는

$$E : y^2 \quad = \quad x^3 + ax + b, a, b \in K \tag{2.11}$$

이 되고 $a_1 = a_2 = a_3 = 0$이 되도록 Weiestrass 방정식을 항상 선택할 수 있다.

만일 E/K가 식(2.11)으로 주어진 타원 곡선이라고 하면 관련된 값으로

$$\Delta = -16(4a^3 + 27b^2)$$

그리고

$$j(E) = -1728(4a)^3/\Delta$$

가 된다.

E가 non-singular라고 하면 $\Delta \neq 0$이 된다. 정리(2.2)를 특별화하면 다음의 결과를 얻는다.

정리 2.6 *타원 곡선 $E_1/K : y^2 = x^3 + ax + b, E_2/K : y^2 = x^3 + \overline{a}x + \overline{b}$가 K상에서 동형이 될 필요 충분 조건은 K^* 상에 u가 존재하여 $u^4\overline{a} = a$와 $u^6\overline{b} = b$이다. 만일 K상에 $E_1 \cong E_2$ 이면, 동형 사상은*

$$\phi : E_1 \to E_2, \phi : (x, y) \mapsto (u^{-2}x, u^{-3}y),$$

이고

$$\psi : E_2 \to E_1, \psi : (x, y) \mapsto (u^2x, u^3y).$$

이다

덧셈 공식

만일 $P = (x_1, y_1) \in E$ 이면 $-P = (x_1, -y_1)$이다. 만일 $Q = (x_2, y_2) \in E$, $Q \neq -P$이면 $P + Q = (x_3, y_3)$은 다음과 같다.

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

단,

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{if } P = Q \end{cases}$$

예 2.1 *Z_{11} 상에 방정식 $E : y^2 = x^3 + x + 6$ 은 타원 곡선을 정의한다. 왜냐하면 $\Delta = 4 \neq 0$이기 때문이다. E상의 유리수 점은*

$$E(Z_{11}) = \{\mathcal{O}, (2,4), (2,7), (3,5), (3,6), (5,2), (5,9), (7,2), (7,9), (8,3), (8,8), (10,2), (10,9)\}$$

이고, 덧셈 규칙을 적용하면 $(2,4) + (2,7) = \mathcal{O}$, $(2,4) + (3,5) = (7,2)$, $(2,4) + (2,4) = (5,9)$ 이다.

제 5 절 표수가 2인 K상의 곡선

K를 표수가 2인 체이고 E/K는 다음의 Weierstrass 방정식으로 주어지는 타원 곡선이라고 한다.

$$E : y^2 + \overline{a}_1 xy + \overline{a}_3 y = x^3 + \overline{a}_2 x^2 + \overline{a}_4 x + \overline{a}_6$$

$j-$불변량은 $j(E) = (\overline{a}_1)^{12}/\Delta$가 된다.

만일 $j(E) \neq 0$ $(\overline{a}_1 \neq 0)$, 허용하는 변수 변환은

$$(x, y) \rightarrow (\overline{a}_1^2 x + \frac{\overline{a}_3}{\overline{a}_1}, \overline{a}_1^3 y + \frac{\overline{a}_1^2 \overline{a}_4 + \overline{a}_3^2}{\overline{a}_1^3})$$

이 E를 다음과 같이 변환한다.

$$E_1/K : y^2 + xy \;\; = \;\; x^3 + a_2 x^2 + a_6 \tag{2.12}$$

이 때, $\Delta = a_6$이고 $j(E) = 1/a_6$가 된다.

만일 $j(E) = 0$ (즉, $\overline{a}_1 = 0$)이면, 허용하는 변수 변환은

$$(x, y) \rightarrow (x + \overline{a}_2, y)$$

이 E를 다음으로 변환한다.

$$E_2/K : y^2 + a_3 y \;\; = \;\; x^3 + a_4 x + a_6 \tag{2.13}$$

E_2에 대하여는 $\Delta = a_3^4$와 $j(E_2) = 0$이다.

$j(E) \neq 0$ 일 때 덧셈 공식

$P = (x_1, y_1) \in E_1$이라 하고, $-P = (x_1, y_1 + x_1)$이다. 만일 $Q = (x_2, y_2) \in E_1$이고 $Q \neq P$이면 $P + Q = (x_3, y_3)$은 다음과 같다.

$$x_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + \dfrac{y_1 + y_2}{x_2 + x_1} + x_1 + x_2 + a_2 & P \neq Q \\ \\ x_1^2 + \dfrac{a_6}{x_1^2} & P = Q \end{cases}$$

그리고

$$y_3 = \begin{cases} (\dfrac{y_1+y_2}{x_1+x_2})(x_1+x_3)+x_3+y_1 & P \neq Q \\ \\ x_1^2+(x_1+\dfrac{y_1}{x_1})x_3+x_3 & P = Q \end{cases}$$

$j(E) = 0$ **일 때 덧셈 공식**

$P = (x_1, y_1) \in E_2$이라 하고, $-P = (x_1, y_1 + a_3)$이다. 만일 $Q = (x_2, y_2) \in E_2$이고 $Q \neq P$이면 $P + Q = (x_3, y_3)$은 다음과 같다.

$$x_3 = \begin{cases} (\dfrac{y_1+y_2}{x_1+x_2})^2+x_1+x_2 & P \neq Q \\ \\ \dfrac{x_1^4+a_4^2}{a_3} & P = Q \end{cases}$$

그리고

$$y_3 = \begin{cases} (\dfrac{y_1+y_2}{x_1+x_2})(x_1+x_3)+y_1+a_3 & P \neq Q \\ \\ (\dfrac{x_1^2+a_4}{a_3})(x_1+x_3)+y_1+a_3 & P = Q \end{cases}$$

제 6 절 군 구조

E를 F_q 상에서 정의된 타원 곡선이라고 하자. 그리고, $q = p^m$ 이고 소수 p는 F_q의 표수라고 하자. $E(F_q)$ 상의 점의 수를 $\#E(F_q)$ 로 표기하자.

만일 E가 식(2.1)으로 주어진다면, $x \in F_q$에 대하여 각 방정식은 2개의 해를 가질 것이므로, $\#E(F_q) \leq 2q+1$ 이다. 직관적으로 보아서, 식(2.1)는 확률 1/2로 F_q 상에 해를 가질 것이다. 따라서 $\#E(F_q) \approx q$ 일 것이다. 다음의 정리는 이것이 맞다는 것을 확인한다.

정리 2.7 *(Hasse) 만일* $\#E(F_q) = q+1-t$*이면* $|t| \leq 2\sqrt{q}$ *이다.*

Hasse 정리의 주요한 결과로 우리는 $E(F_q)$의 타원 곡선 상에 점 P를 확률적으로 다항식 시간내에 균일하고 랜덤하게 선택할 수 있다는 것이다. 이것은 다음과 같이 하면 된다. 우선 임의의 점 $x_1 \in F_q$를 선택한다. x_1이 $E(F_q)$ 상의 임의의 점의 x 좌표이라면, F_q 상에서 y에 관한 근을 계산하여 $(x_1, y_1) \in E(F_q)$이

되도록 y_1을 계산한다. F_q 상에서 확률적인 다항식 시간 내에 근을 찾는 방법은 여러가지[10]가 있다. 만일 곡선의 방정식이 식(2.11)이라면 $P = (x_1, y_1)$ 또는 $(x_1, -y_1)$으로 설정한다. (또는 식(2.12), 식(2.13) 을 가진 다면 각각 $P = (x_1, y_1)$ 또는 $(x_1, y_1 + x_1)$ $P = (x_1, y_1)$ 또는 $(x_1, y_1 + a_3)$가 된다.)

Hasse의 정의에 의하면 x_1이 $E(F_q)$ 상에 어떤 점의 x 좌표가 될 확률은 적어도 $1/2 - 1/\sqrt{q}$ 이다. 지금의 방법으로 위수가 2인 점을 선택할 확률은 다른 점을 선택할 확률보다 2배나 되는 것을 주의하자. 그러나, 이것은 위수가 2인 점이 최대 3개가 있으므로 문제가 되지 아니한다.

다음의 결과는 Waterhouse[152]에 의한 것으로 E가 $q = p^m$인 F_q 상에서 정의한 모든 타원 곡선 상에 변화할 때 $\#E(F_q)$의 가능한 값을 결정한다.

보조정리 2.1 *다음은 $E(F_q)$가 F_q상에 위수가 $q+1-t$를 가지는 타원 곡선E/F_q이 존재할 필요 충분 조건이다.*

(i) $t \not\equiv 0 \pmod{p}$ *그리고* $t^2 \leq 4q$

(ii) m*은 홀수이고 다음의 한 조건을 만족한다.*

(1) $t = 0$

(2) $t^2 = 2q$ *그리고* $p = 2$

(3) $t^2 = 3q$ *그리고* $p = 3$

(iii) m*은 짝수이고 다음의 한 조건을 만족한다.*

(1) $t^2 = 4q$

(2) $t^2 = q$ *그리고* $p \not\equiv 1 \pmod{3}$

(3) $t = 0$ *그리고* $p \not\equiv 1 \pmod{4}$

만일 $q = p$ 가 소수라면, $|t| \leq 2\sqrt{p}$인 모든 t에 대하여 $\#E(F_p) = p + 1 - t$인 F_p 상에 정의되는 타원 곡선 E가 적어도 하나는 존재한다는 것을 주의하자.

사실은 E가 F_q 상의 타원 곡선으로 변화할 때, $\#E(F_p)$ 값은 $p+1$에 중심값으로 하고 $\sqrt{p}$ 값 만큼의 사이를 균일하게 분포할 것이다. 이것은 다음의 증명으로 명확하여 지며 Lenstra의 타원 곡선을 이용한 소인수 분해 방법[80]에 중요한 요소이다.

정리 2.8 *양수의 계산 가능한 상수 c_1과 c_2가 존재하여 $p \geq 5$인 소수와 구간 $[p+1-\sqrt{p}, p+1+\sqrt{p}]$ 상에 있는 정수의 부분 집합 S에 대하여 랜덤한 쌍 $(a,b) \in F_p \times F_p$가 $\#E(F_p) \in S$ 인 타원 곡선 $E : y^2 = x^3 + ax + b$를 정의하는 확률 r_S는 다음과 같이 제한되어 있다.*

$$\frac{\#S-2}{2\lfloor\sqrt{p}\rfloor+1} \cdot c_1(\log p)^{-1} \quad \leq r_S \leq \quad \frac{\#S}{2\lfloor\sqrt{p}\rfloor+1} \cdot c_2(\log p)(\log\log p)^{-2}$$

타원 곡선 E는 $\#E(F_q) = q+1-t$에서 만일 p가 t를 나눈다면 supersingular 라고 한다. 그렇지 아니하면 non-supersingular라고 한다. $p = 2, 3$에서 E는 $j(E)$값이 0이 되면 supersingular 이다. Lemma (2.1)에서 다음을 추출할 수 있다.

따름정리 2.1 *E가 F_q 상에 정의된다면, $t^2 = 0, q, 2q, 3q, 4q$이면 E는 supersingular가 된다.*

다음의 정리는 $E(F_q)$의 군의 형태를 주어진다. n개의 원소를 가진 순환군을 Z_n(또는 Z/n) 아벨 군 론에서 기본적인 결과를 우선 가지고 온다. 모든 유한 아벨 군 G는 순환군의 직합(direct sum)으로 분해될 수 있다.

$$G \quad = \quad Z_{n_1} \oplus Z_{n_2} \oplus \cdots Z_{n_s}$$

여기서 모든 $i = 1, 2, \ldots, s-1$에 대하여 $n_{i+1} | n_i$이고 $n_s \geq 2$이다 또한, 다음의 의미에서 유일하다. 만일

$$G \quad = \quad Z_{m_1} \oplus Z_{m_2} \oplus \cdots Z_{m_t}$$

이 모든 $i = 1, 2, \ldots, t, m_t \geq 2$에 대하여 $m_{i+1} | m_i$이면 순환 군의 또다른 분해로 되면 $s = t$이고 각각의 $i = 1, 2, \ldots, s$에 대하여 $n_i = m_i$이다. 그리고 G는 type $(n_1, n_2, \ldots, n_s)$이고 rank가 s이라고 부른다.

정리 2.9 *$E(F_q)$는 rank가 1 또는 2인 아벨 군이다. 군의 type는 (n_1, n_2)이다. 즉, $E(F_q) \cong Z_{n_1} \oplus Z_{n_2}$이고 $n_2 | n_1$과 $n_2 | q-1$ 이다.*

만일 E가 supersingular 곡선이라면 $E(F_q)$의 군 구조는 다음의 결과에 의하여 결정된다.

보조정리 2.2 *([137]) $\#E(F_q) = q+1-t$라 하면*

(i) 만일 $t^2 = q, 2q, 3q$이면 $E(F_q)$는 순환군이다.

(ii) 만일 $t^2 = 4q$이면 $t = 2\sqrt{q}$ 또는 $t = -2\sqrt{q}$에 각각 $E(F_q) \cong Z_{\sqrt{q}-1} \oplus Z_{\sqrt{q}-1}$ 또는 $E(F_q) \cong Z_{\sqrt{q}+1} \oplus Z_{\sqrt{q}+1}$ 이다.

(iii) 만일 $t = 0$이고 $q \not\equiv 3 \pmod 4$이면 $E(F_q)$는 순환군이다. 만일 $t = 0$와 $q \equiv 3 \pmod 4$이면 $E(F_q)$가 순환군이거나 $E(F_q) \cong Z_{(q+1)/2} \oplus Z_2$ 가 된다.

만일 l가 소수라면, $v_l(n)$을 $l^{v_l(n)}|n$ 인 가장 큰 정수라고 하자. 정리 (2.9)으로 부터 $\#E(F_q) = N$이면 군 $E(F_q)$는 다음의 구조를 가진다.

$$Z/p^{v_p(N)} \oplus \oplus_{l \neq p}(Z/l^{a_l} \oplus Z/l^{b_l}) \tag{2.14}$$

여기서 $a_l \geq b_l$, $a_l + b_l = v_l(N)$, $b_l \leq v_l(q-1)$이다. 예를들면, $\gcd(N, q-1) = 1$이면, $E(F_q)$는 순환군이다. 또한, $N = \#E(F_q)$가 유일한 소수로 인수분해가 되면 $E(F_q)$는 순환군이다.

다음의 보조정리는 F_q 상에 정의되는 모든 non-supersingular 곡선으로 E가 변화할 때 가능한 모든 군 $E(F_q)$를 결정한다.

보조정리 2.3 *([132, 150]) $t \not\equiv 0 \pmod p$, $t^2 \leq 4q$ 일 때 $N = q + 1 - t$라 하자. 만일 $a_l > b_l, a_l + b_l = v_l(N)$이고 모든 소수 $l \neq p$에서 $b_l \leq v_l(q-1)$을 만족하는 정수 a_l, b_l이 있다면, $E(F_q)$가 군 구조로 식(2.14)을 갖는 F_q 상에 non-supersingular 곡선 E가 존재한다.*

곡선 E는 F_q의 확정 체 $L = F_{q^k}$ 상의 타원 곡선으로 볼수 있다. 즉, $E(F_q)$는 $E(L)$의 부분 군이다. 다음의 Weil 정리에 의하면 (1943년에 Hasse가 증명함) $\#E(F_q)$로 부터 $k \geq 2$인 $\#E(F_{q^k})$를 계산할 수 있다.

정리 2.10 *E를 F_q상에 정의된 타원 곡선이고 $t = q+1-\#E(F_q)$이라 하자. 그러면,$\#E(F_{q^k}) = q^k+1-\alpha^k-\beta^k$이고 여기서 α, β는 $1-tT+qT^2 = (1-\alpha T)(1-\beta T)$가 되는 복소수 값이다.*

그러면 $E = E(\overline{F}_q)$인 군 구조에 관한 결과를 언급한다. E는 torsion 군이다. 즉, 각 점 $P \in E$에 대하여 양의 정수 k가 있어 $kP = \mathcal{O}$를 만족한다. 그러한 가장 적은 정수를 P의 위수 (order)라고 한다. *n-torsion* 점은 $nP = \mathcal{O}$를 만족하

는 점 $P \in E(\overline{F}_q)$이다. $E(F_q)[n]$는 $n \neq 0$인 $E(F_q)$상에서 *n-torsion* 점들의 부분군으로 하자.

$E(\overline{F}_q)[n]$를 $E[n]$으로 표기하자. 만일 n과 p가 서로 소라면, $E[n] \cong Z_n \oplus Z_n$이다 만일 $n = p^e$라면, E가 supersingular이면 $E[p^e] \cong \{\mathcal{O}\}$이고 E가 non-supersingular이면 $E[p^e] \cong Z_{p^e}$이다.

예 2.2 *타원 곡선 $E/F_q : y^2 = x^3 + ax + b$이고 $char(F_q) \neq 2, 3$이라 하자. 임의의 점 P는 만일 $P = -P = (x, -y)$이면 위수 2를 갖는다. 즉, $y = 0$이다. x_1, x_2, x_3가 3차 방정식 $x^3 + ax + b$의 근이라면 ($\Delta \neq 0$이면 x_1, x_2, x_3는 각각 다른 값을 갖는다.) 따라서,*

$$E[2] \;=\; \{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\}$$

예 2.3 *q를 $q \equiv 2 \pmod 3$을 만족하는 홀수 소수의 멱이라고 하자. $b \in F_q, b \neq 0$이라 하고, 타원 곡선 $E_1/F_q : y^2 = x^3 + b$를 생각하자. $q \equiv 2 \pmod 3$이므로 사상 $x \mapsto x^3 + b$는 F_q상의 permutation이다. $x^3 + b$이 F_q 상의 (영이 아닌) quadratic residue가 되는 각각의 (q-1)/2 개의 요소 $x \in F_q$은 $E_1(F_q)$에 2 개 점의 x 좌표이다. 즉, $(x, \pm\sqrt{x^3 + b})$이다. $E_1(F_q)$ 상의 다른 점은 $(\sqrt[3]{-b}, 0)$와 $\mathcal{O}$이므로 $\#E_1(F_q) = q + 1$이고 E_1은 supersingular이다.*

보조정리 (2.2)의 (iii)에 의하면 $E_1(F_q)$의 군 type의 2가지 가능성은 $((q + 1)/2, 2)$와 $(q + 1)$이다. $E_1(F_q)$상에서 유일한 2-torsoin 점은 $\mathcal{O}$와 $(\sqrt[3]{-b}, 0)$이고 $E_1(F_q)[2] \cong Z_2$이다. 따라서, $E_1(F_q)$는 위수 $q + 1$의 순환 군이다.

예 2.4 *q를 $q \equiv 3 \pmod 4$을 만족하는 홀수 소수의 멱이라고 하자. $a \in F_q, a \neq 0$이라 하고, 타원 곡선 $E_2/F_q : y^2 = x^3 + ax$를 생각하자.*

$q \equiv 3 \pmod 4$이므로 -1은 F_q 상에서 quadratic non-residue이다. $(-x)^3 + a(-x) = -(x^3 + ax)$가 됨을 관찰한다. $x^3 + ax \neq 0$인 각 $x \in F_q$에 대하여 $x, -x$ 중 하나는 $E_2(F_q)$ 상에서 2 점의 x 좌표가 된다. 만일 $x \in F_q, x \neq 0$이 $x^3 + ax = 0$를 만족하면, $(x, 0)$, $(-x, 0)$는 $E_2(F_q)$상의 2 점이다. (0,0과 $\mathcal{O}$를 함께 $E_2(F_q)$ 상의 위수는 $q + 1$이고 E_2는 supersingular이다.

E_2에는 위수가 2인 3개의 점이 있다. 즉, $P_1 = (0, 0), P_2 = (\sqrt{-a}, 0), P_3 = (-\sqrt{-a}, 0)$이다. 만일 $\sqrt{-a} \in F_q$이면 즉, a가 F_q의 quadratic non-residue이면 P_2와 P_3는 $E_2(F_q)$에 존재한다. 만일 a가 F_q상의 quadradic residue이면 $E_2(F_q)$는 순환한다. 반면 $E_2(F_q)$는 만일 a가 F_q 상에 quadratic non-residue 이면 type $((q+1)/2, 2)$를 갖는다.

타원 곡선과 관계가 있는 *division polynomial*을 정의하자. E/F_q를 $char(F_q) \neq 2, 3$인 타원 곡선 $y^2 = x^3 + ax + b$라 하자. $n \geq 0$에서 다항식 $\Psi_n(x, y) \in F_q[x, y]$를 다음과 같이 정의하자.

$$\begin{aligned}
\Psi_0(x,y) &= 0 \\
\Psi_1(x,y) &= 1 \\
\Psi_2(x,y) &= 2y \\
\Psi_3(x,y) &= 3x^4 + 6ax^2 + 12bx - a^2 \\
\Psi_4(x,y) &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3) \\
\Psi_{2n+1}(x,y) &= \Psi_n(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2)/2y, \qquad n \geq 2 \\
\Psi_{2n}(x,y) &= \Psi_{n+2}\Psi_n^3 - \Psi_{n+1}^3\Psi_{n-1}, \qquad n \geq 3
\end{aligned}$$

각 Ψ_n은 $F_q[x, y]$에서 다항식이 되는 것을 n에 대하여 induction을 하면 구해지는 것을 쉽게 알 수 있다. Ψ'_n을 Ψ_n에서 y^2를 $x^3 + ax + b$로 반복적으로 대체한 다항식이라고 하자. 만일

$$f_n = \begin{cases} \Psi'_n(x,y) & \text{if } n \text{ is odd} \\ \Psi'_n(x,y)/y & \text{if } n \text{ is even} \end{cases}$$

로 정의하면 $f_n \in F_q[x]$이다. 다음은 E의 n-torsion 점을 구하는 데 division polynomial의 유용성을 나타낸다.

정리 2.11 *$P = (\overline{x}, \overline{y}) \in E\backslash\{\mathcal{O}\}$ 라 하자.*

(i) $\Psi_n(x, y) = 0$ *이면* $P \in E[n]$*이다. 즉, E상에 다항식 Ψ_n는 영이 아닌 n-torsion 점에 근을 가지고 있다.*

(ii) *만일* $P \notin E[2]$ *이면* $f_n(\overline{x}) = 0$*이어야 만* $P \in E[n]$*이다. (즉, f_n의 근은 $E[2]$에 있지 않는 n-torsoin 점의 정확하게 x 좌표가 된다.)*

(iii) *만일* $P \notin E[n]$*이면*

$$nP = (\overline{x} - \frac{\Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2}{4\overline{y}\Psi_n^3})$$

여기서 Ψ_k는 $\Psi_k(x, y)$를 의미한다.

제 7 절 Divisor 이론

Divisor는 유리 함수에서 영점(zero)와 극점(pole)을 조사하는 데 유용하다. 5 장에서 타원 곡선에서 이산 대수 문제를 어떤 유한체에서 이산 대수 문제로 축약하는 데 이용된다. 이 절에서 거론한 결과의 기초적인 증명은 [26]을 참조하라.

$K = F_q$, E/F_q를 타원 곡선이라고 하자. *divisor* D는 $\overline{F}_q$ 점들의 formal sum이다.

$$D = \sum_{P \in E} n_P(P)$$

여기서 $n_P \in Z$ 이고 모든 그리고 유한적으로 많은 $P \in E$에 대하여 $n_P = 0$이다. $supp(D)$로 표시하는 divisor D의 *support*는 $\{P \in E | n_P \neq 0\}$ 점의 집합이다.

모든 divisor의 집합은 **D**로 표시하면 군을 형성하는 데 덧셈은

$$\sum_{P \in E} n_P(P) + \sum_{P \in E} m_P(P) = \sum_{P \in E} (n_P + m_P)(P)$$

D는 E의 점에 의하여 생성된 아벨 군이다.

Divisor $D = \sum n_P(P)$의 차수는 $deg(D) = \sum n_P$이다. D^0를 차수 0인 모든 divisor의 집합으로 표기한다. 그러면 D^0는 D의 부분 군이 된다.

만일 E가 다음의 (아핀) Weierstrass 방정식으로 정의된다면

$$r(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

단, $r \in K[x, y]$이고, K위의 E의 coordinate ring을 $K[E]$로 표시하면 이것은 integral domain이 된다.

$$K[E] = K[x, y]/(r)$$

단, (r)은 r에 의하여 발생된 $K[x, y]$에 있는 ideal을 의미한다. 유사하게

$$\overline{K}[E] = \overline{K}[x, y]/(r)$$

를 정의한다. 각 $l \in \overline{K}[E]$에 대하여 y^2에 $y^2 - r(x, y)$로 반복적으로 대체하면 다음을 구한다.

$$l(x, y) = v(x) + yw(x), \text{ where } v(x), w(x) \in \overline{K}(x)$$

K 상의 function field $K(E)$는 $K[E]$의 부분들의 함수이다. (만일 I가 Integral domain이면 그것의 부분들의 함수 F는 몫 $a/b, a, b \in I, b \neq 0$ 의 등가 류들의

집합이 된다. F의 덧셈과 곱셈은 자연스럽게 정의된다는 것을 상기하자). 유사하게 $\overline{K}$ 상의 E의 function field인 $\overline{K}(E)$는 그것의 부분들의 field이다. $\overline{K}[E]$의 요소를 유리 함수 (rational function) 라고 하고 $\overline{K}$는 $\overline{K}(E)$의 준 체 (subfield)이다.

$f \in \overline{K}(E)^*$ 을 영이 아닌 유리함수라고 하고 $P \in E\backslash\{\mathcal{O}\}$라 하자. 그러면 $f(P) \neq 0$이고 $g, h \in \overline{K}[E]$에 대하여 $f = g/h$로 표시될 수 있다면 f는 P에서 정의된다 (defined at P)고 한다. 만일 f가 P에서 정의된다면, $f(P) = g(P)/h(P)$로 놓는다. 이것은 well-defined 된 것을 쉽게 알 수 있다. 즉, $f(P)$의 값은 g와 h의 값에 의존하지 아니한다. 만일 $f(P) = 0$이면, f는 P에서 영점을 가졌다고 하고 만일 f가 P에서 정의되지 아니 한다면, f는 P에서 극점을 가졌다고 하고 $f(P) = \infty$라고 쓴다.

예 2.5 *$char(K) \neq 2, 3$인 유한 체 $K = F_q$상에 타원 곡선 $E : y^2 = x^3 - x$를 생각하자. $P = (1, 0) \in E$로 하고 $f = (x^2 - x)/y \in \overline{K}(E)$로 놓자.*

만일 f를 다항식의 몫, 즉 $f \in \overline{K}(x, y)$로 생각하면 f는 P에서 정의되지 아니한다. 그러나, $\overline{K}(E)$의 요소로 생각하면

$$f = \frac{(x^2 - x)}{y} = \frac{(x^2 - x)y}{y^2} = \frac{(x^2 - x)y}{x^3 - x} = \frac{y}{x + 1}$$

로 $f(P) = 0$이 된다.

점 $\mathcal{O}$에서 f 값을 정의하는 데는 [26]에서 취한 방법을 따른다. $l \in \overline{K}[E]$에 대하여 $l(x, y) = v(x) + yw(x)$로 쓸 수 있다. 여기서 $v(x), w(x) \in \overline{K}[x]$이다. x에 2의 무게를 두고, y에 3의 무게를 두자. l의 차수는 다음과 같이 정의한다.

$$Deg(l) = \max(2 \deg_x(v), 3 + 2 \deg_x(w)).$$

$g, h \in \overline{K}[x, y]/(r)$에서 $f = g/h$로 놓는다. 만일 $Deg(g) < Deg(h)$이면 $f(\mathcal{O}) = 0$이다. 만일 $Deg(g) > Deg(h)$이면 $f(\mathcal{O}) = \infty$이다. 만일 $Deg(g) = Deg(h)$이면 g와 h에서 최고차항이 각각 ax^d, bx^d이므로 $f(\mathcal{O}) = a/b$이다. 그렇지 아니하면, 최고차항이 cyx^d와 dyx^d이므로 $f(\mathcal{O}) = c/d$이다.

예 2.6 *타원곡선 $E : y^2 = x^3 + ax + b$를 생각하자. $f = y, g = x/y, h = (x^2 - xy)/(1 + xy) \in \overline{K}[E]$로 하면 $f(\mathcal{O}) = \infty, g(\mathcal{O}) = 0, h(\mathcal{O}) = -1$이다.*

각 점 $P \in E$에 대하여 유리함수 $u \in \overline{K}(E), u(P) = 0$가 존재하여 만일 $f \in \overline{K}(E)^*$이면 $f = u^d s$로 쓸 수 있고 여기서 $s \in \overline{K}(E), s(P) \neq 0, \infty$이다. 정수 d는 u 값에 의존하지 아니한다. 함수 u를 P에 대하여 균일 변수 (uniformizing parameter)라고 부른다. 다음 결과[44, p.70]는 균일 변수를 찾는 데 도움이 된다.

정리 2.12 *$P \in E$로 놓자. 만일 $l : ax + by + c = 0$이 P에서 E의 접선이 아닌 P를 지나는 어떠한 선이라면 l은 P에 대하여 균일 변수이다.*

예 2.7 *$char(K) \neq 2, 3$인 유한체 $K = F_q$상에서 타원 곡선 $E : y^2 = x^3 + ax + b$를 생각하자.*

- *$P = (c, d) \notin E[2]$이고 P에서 E의 접선*

$$(-3c^2 - a)(x - c) + 2d(y - d) = 0$$

이다. $d \neq 0$이므로, P에 대한 균일 변수는 $u = x - c$이다.

- *$P = (c, 0) \in E$는 위수 2의 점이다. P에서 E의 접선은*

$$(-3c^2 - a)(x - c) = 0$$

이다. $u = y$는 P에 대한 균일 변수이다.

- *$\mathcal{O}$에 대한 균일 변수를 찾기 위하여는 다른 좌표 계에서 작업을 하여야 한다. E에 대한 homogeneous 방정식이 $Y^2Z = X^3 + aXZ^2 + bZ^3$을 상기하자. 아핀 좌표 $u = X/Y, w = Z/Y$로 하면 방정식은 $f(u, w) = vm^3 + avw^2 + bw^3 - w = 0$이 된다. 그러면, $\frac{\delta f}{\delta v}(\mathcal{O}) = 0$, $\frac{\delta f}{\delta w}(\mathcal{O}) = -1$이 된다. $\mathcal{O}$에서 E로 접선의 방정식은 $w = 0$이다. 선분 $v = 0$는 $\mathcal{O}$을 지나지만 $\mathcal{O}$에서 접선은 아니다. 원래의 (x, y) 좌표에서 $u = x/y$는 cl에 대하여 균일 변수이다.*

$f \in \overline{K}(E), P \in E$이라고 하자. $f = u^d s$라고 하면 u는 $P, s \in \overline{K}(E)$에 대하여 임의의 균일 변수이고 $s(P) \neq 0, \infty$이다. P에서 f의 위수(order)는 d에서 정의될 수 있다. 이 때를 $\mathrm{ord}_P(f) = d$로 표기한다. 점 P는 $\mathrm{ord}_P(f) > 0$일 때만 f의 영점으로 되도 이 경우 배수(multiplicity)는 $\mathrm{ord}_P(f)$로 정의된다. 유사하게 점 P는 $\mathrm{ord}_P(f) < 0$이면 극점을 가지게 되고 이 때 배수는 $-\mathrm{ord}_P(f)$가 된다. 함수

f가 E 상에서 유한의 영점과 극점을 가지므로 $\mathrm{div}(f)$, f의 divisor를 다음과 같이 정의할 수 있다.

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P)$$

유리함수에 대한 기본 사실은 만일 $f \in \overline{K}(E)^*$이면 $\mathrm{div}(f) \in D^0$이다. 더욱이, $f \in \overline{K}^*$이어야만 $\mathrm{div}(f) = 0$이다.

예 2.8 *$char(K) \neq 2, 3$인 유한체 $K = F_q$상에서 타원 곡선 $E : y^2 = x^3 + ax + b$를 생각하자.*

- *$P = (c, d) \notin E[2]$이라 하자. 그러면*

$$div(x - c) = (P) + (-P) - 2(\mathcal{O}).$$

- *$P_1, P_2, P_3 \in E$ 가 위수 2의 점이라 하자.*

$$div(y) = (P_1) + (P_2) + (P_3) - 3(\mathcal{O}).$$

- *$b \neq 0$이고 $P_4 = (0, \sqrt{b}), P_5 = (0, -\sqrt{b})$ 라 하자. 그러면*

$$div(\frac{x}{y}) = (P_4) + (P_5) + (\mathcal{O}) - (P_1) - (P_2) - (P_3)$$

임의의 $f \in \overline{K}(E)^*$에 대하여 만일 $D = \mathrm{div}(f)$이면 divisor $D \in D^0$는 principal이라 한다. 다음은 principal divisor에 대한 중요한 특징이다.

정리 2.13 *$D = \sum n_P(P)$는 divisor이다. 그러면 $\sum n_P = 0$ 과 $\sum n_P P = \mathcal{O}$이면 D는 principal이다.*

D_l을 principal divisor의 모든 집합이라고 하자. 만일 $f_1, f_2 \in \overline{K}(E)$이면 $\mathrm{div}(f_1 f_2) = \mathrm{div}(f_1) + div(f_2)$이다. 이것은 D_l이 D^0의 부분 군을 형성한다. quotient group D^0/D_l은 E의 (영 부분의) divisor class group 또는 Picard group이라고 한다.

만일 $D_1 - D_2 \in D_l$ 즉, 어떤 $f \in \overline{K}(E)$에서 $D_1 = D_2 + \mathrm{div}(f)$ 될 때 2개의 divisor, $D_1, D_2 \in D^0$ 는 등가라고 하고 $D_1 \sim D_2$라고 표기한다. 각 $D \in D^0$에 대하여 유일한 점 $Q \in E$가 존재하여 $D \sim (Q) - (\mathcal{O})$이다. 사실, 만일 $D = \sum n_P(P)$이면 $Q = \sum n_P P$이다. $\sigma : D^0 \to E$는 이러한 사상을 의미한다면 σ는 군 D^0/D_l과 E간의 동형 사상 (isomorphism)을 유발한다.

제 8 절 Z_n 상의 타원 곡선

환 Z_n 상에서의 타원 곡선의 개념을 정의하자. Z_n 상의 타원곡선은 Lenstra의 소인수 분해 알고리즘 [80]과 Goldwasser-Kilian의 소수 판정 알고리즘[48]에 이용된다.

n을 $\gcd(n,6)=1$인 양의 정수로 하자. Z_n 상의 타원 곡선은 다음의 방정식으로 주어진다.

$$E_{a,b}: y^2 = x^3 + ax + b \tag{2.15}$$

여기서 $a,b \in Z_n$이고 $\gcd(4a^3+27b^2,n)=1$이다. $E_{a,b}(Z_n)$으로 표기하는 $E_{a,b}$상의 점은 무한원점 $\mathcal{O}$를 포함하여 식 (2.15)의 $Z_n \times Z_n$에서 해의 집합이다. p를 n의 임의의 소수의 divisor라고 하고 $\overline{a}$는 a modulo p를 포함하는 congruence class라고 하자. $E_{\overline{a},\overline{b}}$는 F_p상에서 정의된 타원 방정식임을 주의하라. $P \in E(Z_n)$이라 하자.

만일

$$P_P = \begin{cases} (\overline{x},\overline{y}), & \text{if } P=(x,y) \\ \mathcal{O}_p, & \text{if } P=\mathcal{O}_n \end{cases}$$

로 정의하고 $\mathcal{O}_p$를 $E_{\overline{a},\overline{b}}(F_p)$에서 무한 원점이라 하면 $P_P \in E_{\overline{a},\overline{b}}(F_p)$ 이다.

우리는 절 (4)에서 정의한 동일한 덧셈 규칙을 가지고 $E_{a,b}(Z_n)$ 상의 점을 의사 덧셈을 정의하자. 유한체에서 정의한 타원 곡선과 달리 $E_{a,b}(Z_n)$은 이런 덧셈에 대하여 군이 아니다. 덧셈이 반드시 정의되지 아니한 것은 분명하다. 만일 $\gcd(x_2-x_1,n)>1$ (즉, $P \neq Q$ 인 경우) 또는 $\gcd(2y_1,n)>1$ (즉, $P=Q$인 경우)에는 λ에 관한 공식에서 Z_n 상의 가역이 아닌 요소에 의한 나눗셈을 가지고 있다.

의사 덧셈에 관한 다음의 성질은 쉽게 검증할 수 있다.

(i) 만일 $P,Q \in E_{a,b}(Z_n)$이고 $P+Q$가 정의가 되지 아니하면 덧셈 법칙을 시행하면 n의 non-trivial divisor를 생성한다.

(ii) 만일 $P,Q \in E_{a,b}(Z_n)$이고 $P+Q$가 의사 덧셈에 의하여 잘 정의된다면 n의 모든 prime divisors p에 대하여 $(P+Q)_p) = P_p + Q_P$이다.

(iii) 만일 $P \in E_{a,b}(Z_n), k \in Z$이고 kP가 의사 덧셈의 반복 적용에 의하여 잘 정의된다면 n의 모든 prime divisors p에 대하여 $(kP)_p = kP_p$이다.

n이 2개의 소수 p, q의 곱이라고 가정하고

$$\tilde{E}_{a,b}(Z_n) = E_{a,b}(F_p) \times E_{a,b}(F_q)$$

이라 하자.

2개 군의 직접(direct product)이므로 $\tilde{E}_{a,b}(Z_n)$는 군이다. 각 점 $P \in E_{a,b}(Z_n)$은 $\tilde{E}_{a,b}(Z_n)$에 유일한 요소에 상응한다. 즉, (P_p, P_q)이다. $P = \mathcal{O}_p$ 또는 $Q = \mathcal{O}_q$이나 (P, Q가 모두가 $\mathcal{O}$인 영인 경우는 아니지만) 요소 (P, Q)를 제외한 $\tilde{E}_{a,b}(Z_n)$상의 모든 요소를 의미한다. 위의 (ii) 성질에 의하여 정의가 되는 $E_{a,b}(Z_n)$상의 뎃셈은 $\tilde{E}_{a,b}(Z_n)$상의 군 연산과 일치한다.

그러면 소인수 p, q를 모르고도 군 $\tilde{E}_{a,b}(Z_n)$상에서 연산이 가능하다. 군 연산은 성공하거나, 또는 실패하면 n의 non-trivial factor를 얻는다. 만일 p와 q가 크다면, (100 자리 이상이면) n의 소인수는 intractable 문제이다고 믿고 있다. 군 연산이 실패할 경우가 발생할 경우는 극히 드물다고 생각한다.

제 3 장

유한체 상 타원 곡선의 동형 류

본 장에서는 유한체 K상 타원 곡선의 동형류(isomorphism class)를 계수한다. $K = F_{2^m}$ 인 경우, 각 동형류를 Weierstrass 형식으로 대표형을 나열하고 F_{2^m}상에 정의된 각 초특이 타원 곡선 E에 대하여 $\#E(F_{2^m})$을 결정한다.

제 1 절 서론

$(\frac{a}{b})$는 통상의 Jacobi 기호로 표기한다. 그리고 다음을 정의한다.

$$\left(\frac{a}{2}\right) = \begin{cases} 1, & \text{if } a \equiv \pm 1 \bmod 8, \\ 0, & \text{if } a \equiv 0 \bmod 2, \\ -1, & \text{if } a \equiv \pm 3 \bmod 8. \end{cases}$$

Waterhouse[152] (또한 [137])는 우선 어떠한 환이 어떤 타원 곡선의 endormorphism 환으로서 생기는 가를 결정하고 주어진 endormorphism 환에서 타원 곡선의 동형 류의 수를 계수함으로하여 유한체 F_q상에 정의된 타원 곡선의 동형 류의 수를 계산하였다. 그는 또한, F_q 상 동형 류의 수인 $N_q(t)$를 $\#E(F_q) = q + 1 - t$가 되도록 결정하였다. 얻은 결과는 다음과 같다.

정리 3.1 (152) *F_q는 유한체이다. F_q상에 정의된 타원 곡선의 동형 류의 수는 다음과 같다.*

$$N_q = 2q + 3 + (\frac{-4}{q}) + 2(\frac{-3}{q})$$

정리 3.2 *p는 소수이고 $q = p^m$이라 한다. t는 $|t| \leq 2\sqrt{q}$인 정수라고 한다. 그러면*

$$N_q(t) = \begin{cases} H(t^2 - 4q) & \text{if } t^2 < 4q, \text{ and } p \not| t. \\ H(-4q) & \text{if } t = 0 \text{ and } m \text{ odd.} \\ 1 & t^2 = 2q, p = 2, m \text{ odd.} \\ 1 & t^2 = 3q, p = 3, m \text{ odd.} \\ \frac{1}{12}\left(p + 6 - 4(\frac{-3}{p}) - 3(\frac{-4}{p})\right) & t^2 = 4q \text{ and } m \text{ even.} \\ 1 - (\frac{-3}{p}), & \text{if } t^2 = q \text{ and } m \text{ even.} \\ 1 - (\frac{-4}{p}), & \text{if } t = 0 \text{ and } m \text{ even.} \\ 0, & otherwise \end{cases}$$

이다.

$H(\Delta)$는 Δ의 Kronecker class number로, Δ값은 음의 정수로 modulo 4에 0 또는 1을 가지며, 판별식 Δ의 positive definite quadratic form의 $SL_2(Z)$-orbit의 수이다. $H(\Delta)$를 결정하는 방법은 $H(\Delta) = \#\tilde{B}(\Delta)$ 라는 사실에서 구해 진다.

$$\begin{aligned} \tilde{B}(\Delta) &= \{(a,b,c) \in Z^3 : a > 0, b^2 - 4ac = \Delta, |b| \leq a \leq c, \\ &\quad \text{and } b \geq 0 \text{whenever } a = |b| \text{ or } a = c\}. \end{aligned}$$

(만일 $(a,b,c) \in \tilde{B}(\Delta)$이면, $a \leq \sqrt{|\Delta/3}$이고 $\tilde{B}(\Delta)$는 유한 집합이다.) binary quadratic form과 이의 타원 곡선의 endormorphism ring간의 관계는 [137]을 참조)

정리(3.1)의 기본 증명을 제공한다. 정리 (2.2)을 이용하여 동형의 정의로부터 증명을 간단히 할 수 있다. 편리 상 요약한다.

Tr는 Trace 함수로 선형 방정식 $Tr : F_{2^m} \to F_2$를 표기하며 다음과 같이 정의된다.

$$Tr : \alpha \mapsto \alpha + \alpha^{2^1} + \alpha^{2^2} + \cdots \alpha^{2^{m-1}}$$

만일 m이 짝수라면, Te를 함수 $Te : F_{2^m} \to F_4$로 다음과 같이 정의한다.

$$Te : \alpha \mapsto \alpha + \alpha^{2^2} + \alpha^{2^4} + \cdots \alpha^{2^{m-2}}$$

F_4의 원소는 $0, 1, c_1, c_2$로 표기한다. 그러면 항등식 $c_1^2 + c_1 + 1 = 0$, $c_2^2 + c_2 + 1 = 0$, $c_1 c_2 = 0$, $c_1 + c_2 = 1$을 얻는다. $Te(c_1\alpha) = c_1 Te(\alpha)$, $Te(c_2\alpha) = c_2 Te(\alpha)$ 임을 주의한다.

2차 방정식

$$x^2 + ax + b = 0, a, b \in F_{2^m}, a \neq 0$$

는 $Tr(a^{-2}b) = 0$이어야 만 F_{2^m}상에서 해가 있다. 만일 x_1이 하나의 해이면 다른 해는 $x_1 + a$ 가 된다.

유한체에서 아핀 다항식의 근에 수에 대한 [98]에서 일반적인 결과를 이용하여, 다음의 4차 방정식에서

$$x^4 + ax + b \;\; = \;\; 0, a, b \in F_{2^m}, a \neq 0 \tag{3.1}$$

F_{2^m}상에 해의 수는 다음의 결과를 얻는다.

(i) 만일 m이 홀수이면, 식(3.1)은 해가 없던 가 정확하게 2개의 해를 가진다.

(ii) 만일 m이 홀수이고 a가 3승근(cube)이 아니면 식(3.1)은 정확히 한 개의 해를 가진다.

(iii) 만일 m이 홀수이고 a가 3승근(cube)이면 식(3.1)은 만일 $Te(b/a^{4/3}) = 0$이면 4개의 해를, 만일$Te(b/a^{4/3}) \neq 0$이면 해를 가지지 아니한다.

제 2 절 $char(F_q) \neq 2,3$인 F_q 상에 곡선의 동형 류

$E_1/F_q : y^2 = x^3 + ax + b$, $E_2/F_q : y^2 = x^3 + \overline{a}x + \overline{b}$는 2개의 타원 곡선으로 F_q에서 동형이라고 하자. 정리(2.6)에 의하여 $u^4\overline{a} = a$와 $u^6\overline{b} = b$ 방정식에 $u' \in F_q^*$에서 해가 존재한다. 그러한 해 $u \in F_q^*$의 수를 $Aut(E_1)$이라고 표기하고 수를 헤아려 본다. ($Aut(E_1)$은 F_q상에 정의된 E_1의 automorphism의 수이다.) $a = 0$일 때 $\overline{a} = 0$와 $b = 0$일 때 $\overline{b} = 0$인 때를 고려한다. 다음의 3가지 경우가 있다.

(i) 만일 $a \neq 0, b \neq 0$ (그러면 $j(E) \neq 0, 1728$) 이면 $u^2 = \frac{\overline{a}b}{a\overline{b}}$이고 해는 $u \in \{u', -u'\}$이다.

(ii) 만일 $a = 0, b \neq 0$이면 (그러면, $j(E) = 0$) $u^6 = b/\overline{b}$를 얻는다. 만일 F_q^*가 위수 3의 원소 α를 가지고 있다면, 6개의 해 $u \in \{u', \alpha u', \alpha^2 u', -u', -\alpha u', -\alpha u'\}$가 있다. 그렇지 아니하면 $u \in \{u', -u'\}$ 이다.

(iii) 만일 $a \neq 0, b = 0$이면 (그러면, $j(E) = 1728$) $u^4 = a/\overline{a}$를 얻는다. 만일 F_q^*가 위수 4의 원소 β를 가지면, $u \in \{u', \beta u', \beta^2 u', \beta^3 u'\}$ 이며 그렇지 아니하면 $u \in \{u', -u'\}$ 이다.

그러면 허용하는 변수 변환은 $u \in F_q^*$에서 $(x, y) \to (u^2x, u^3y)$의 형태이다. 주어진 곡선 E/E_q에서 동형이 되는 곡선의 수는 $(q-1)/Aut(E)$이다. F_q상에 정의되는 곡선의 수는 q^2-q이다. 왜냐하면, 방정식 $4a^3+27b^2=0$의 해 (a, b)의 수는 q이기 때문이다. 따라서

$$\sum_E \frac{q-1}{Aut(E)} = q^2 - q$$

그리하여

$$\sum_E \frac{1}{Aut(E)} = q$$

이다. 여기서 합은 F_q상에 정의된 타원 곡선의 동형 류의 대표 곡선의 집합이다.

$\gcd(q, 6) = 1$이므로 $q \equiv 1, 5, 7, 11 \pmod{12}$를 얻는다. 그러면 만일 $q \equiv 1, 7 \pmod{12}$이면 F_q^*는 위수 3의 원소를 가진다. 그리고 만일 $q \equiv 1, 5 \pmod{12}$이면F_q^*는 위수 4의 원소를 가진다. 이 사실을 $Aut(E)$의 크기에 대한 결과를 혼합하면 다음의 정리를 얻는다.

정리 3.3 *$char(F_q) > 3$인 유한체 F_q 상에 타원 곡선의 동형 류의 수는 $q = 1, 5, 7, 11 \pmod{12}$에 각각 $2q+6, 2q+2, 2q+4, 2q$이다.*

표 (2)은 체 F_5상에 타원 곡선의 동형 류와 각 곡선의 크기와 군 구조와 함께 제시하였다. 순서 쌍 (a, b)는 곡선 $y^2 = x^3 + ax + b$를 나타낸다

다음은 아벨 군으로 동형이 되는 2개의 비 동형 타원 곡선의 예이다.

예 3.1 *F_5 상에서 $y^2 = x^3 + 1$ 과 $y^2 = x^3 + 2$를 생각하자. 각 곡선은 위수 6을 가진다. 그리고 2개의군은 Z_6에 동형이 된다. 그러나 F_5 상에는 동형이 되지 아니한다. 왜냐하면 $2u^6 = 1$을 만족하는 $u \in F_5^*$가 존재하지 아니한다.*

제 3 절 F_{2^m}상에 비 초특이 곡선의 동형 류

다음의 식으로 E_1과 E_2는 F_{2^m}상에 비 초특이 타원 곡선이라고 하자.

$$E_1 \ : \ y^2 + xy = x^3 + a_2x^2 + a_6 \ (a_6 \neq 0)$$
$$E_2 \ : \ y^2 + xy = x^3 + \overline{a}_2x^2 + \overline{a}_6 \ (\overline{a}_6 \neq 0)$$

정리(2.2)를 특별화하여 만일 반드시 $a_6 = \overline{a}_6\overline{a}_2 = a_2 + s + s^2$인 $s \in F_{2^m}$이 존재하면 $E_1 \cong E_2$임을 알 수 있다. 뒤의 조건은 $Tr(\overline{a}_2 + a_2) = 0$ 즉, $Tr(\overline{a}_2) = Tr(a_2)$임과 동치인 것이다. 이로서 다음의 결과를 얻는다.

표 3.1: F_5상의 타원 곡선의 동형 류

동형 류	점의 수	군 type
(0,1)(0,4)	6	Z_6
(0,2)(0,3)	6	Z_6
(1,0)	4	$Z_2 \oplus Z_2$
(2,0)	2	Z_2
(3,0)	10	Z_{10}
(4,0)	8	$Z_2 \oplus Z_4$
(1,1)(1,4)	9	Z_9
(1,2)(1,3)	4	Z_4
(2,1)(2,4)	7	Z_7
(3,2)(3,3)	5	Z_5
(4,1)(4,4)	8	Z_8
(4,2)(4,3)	3	Z_3

정리 3.4 *$q = 2^m$이고 F_{2^m}상에 비 초특이 타원 곡선은 $2(q-1)$ 개의 동형 류가 있다. γ 는 $Tr(\gamma) = 1$ (만일 m이 홀수이면, $\gamma = 1$로 한다.) 이 되는 원소라 한다. 동형 류의 대표 곡선의 집합은 다음과 같다.*

$$\left\{y^2 + xy = x^3 + a_2x^2 + a_6 | a_6 \in F_{2^m}^*, a_2 \in \{0, \gamma\}\right\}$$

E_1에 동형인 $q/2$ 개의 곡선은 $y^2+xy = x^3+\alpha x^2+a_6$이고 α는 $Tr(\alpha) = Tr(a_2)$를 만족하는 F_{2^m}상 $q/2$개 중 하나이다. 만일 F_{2^m}상에 $E_1 \cong E_2$이면 동형 사상은 $\phi : (x, y) \to (x, y + sx)$로 주어지고 $s^2 + s = a_2 + \overline{a}_2$이다.

제 4 절 홀수 m의 F_{2^m} 상 초특이 타원 곡선의 동형 류

만일 m이 홀수이면, $2^m - 1 \equiv 1 \pmod 3$이다. F_m^*는 위수 3의 원소를 가지고 있지 아니하므로 사상 $f : F_{2^m} \to F_{2^n}$은 전단사인 $f : x \to x^3$으로 정의된다.

E'/F_{2^m}은 다음의 식으로 주어진 곡선이라 하자.

$$E' : y^2 + a_3'y = x^3 + a_4'x + a_6'(a_3' \neq 0.)$$

$r = \sqrt[3]{a_3'}$ 라 하자. 허용하는 변수 변환 $(x, y) \to (r^2x, r^3y)$로 E'은 다음의 곡선으로 변환한다.

$$E \quad : \quad y^2 + y = x^3 + a_4x + a_6 \tag{3.2}$$

홀수 m에 대하여 F_{2^m} 상에 임의의 초특이 타원 곡선이 식 (3.2)와 같은 형태를 가지었다고 가정한다 ; 이런 곡선은 q^2개가 있다. 단 $q = 2^m$이다. 만일 $\overline{E}$가 다음과 같이 주어진다면

$$\overline{E} : y^2 + y = x^3 + \overline{a}_4x + \overline{a}_6$$

정리 (2.2)를 특별화하면 $s, t \in F_{2^m}$이 다음과 같이 존재할 때에만 F_{2^m}상에 $E \cong \overline{E}$이다.

$$s^4 + s + a_4 + \overline{a}_4 = 0 \tag{3.3}$$

$$t^2 + t + s^6 + a_4s^2 + a_6 + \overline{a}_6 = 0 \tag{3.4}$$

허용하는 변수 변환은 $(x, y) \to (x + s^2, y + sx + t)$의 형태를 가지고 $s, t \in F_{2^m}$이다.

E_1을 곡선

$$E_1 : y^2 + y = x^3$$

이라 하자. F_{2^m}상에 $E \cong E_1$이라 가정한다. 그러면 $s_1, t_1 \in F_{2^m}$이 존재하여 다음의 방정식을 만족한다.

$$s^4 + s + a_4 = 0 \tag{3.5}$$

$$t^2 + t + s^6 + a_6 = 0 \tag{3.6}$$

m이 홀수이므로 식 (3.5)는 F_{2^m}에 정확히 2개의 해 즉, s_1과 $s_1 + 1$을 가진다. (s_1, t_1)이 식 (3.6)의 해이므로 $Tr(s_1^6 + a_6) = 0$을 가진다. 그리고 식 (3.5)와 (3.6)을 만족하는 (s, t)가 정확히 2개의 해를 가지므로 $Tr((s_1 + 1)^6 + a_6) = 1$ 이다. 허용하는 변수 변환이 q^2이 있으므로 E_1에 동형인 $q^2/2$ 곡선이 있다는 것을 결론 지을 수 있다.

E_2는 곡선

$$E_2 : y^2 + y = x^3 + x$$

라고 하자. $Tr(s^4+s)=0$이고 $Tr(1)=1$이므로 F_{2^m} 상에 해가 없어 F_{2^m} 상에 $E_1 \ncong E_2$이다. 만일 F_{2^m} 상에 $E \cong E_2$이면 다음의 식을 만족하는 $s_1, t_1 \in F_{2^m}$이 존재한다.

$$s^4+s+1+a_4 = 0 \tag{3.7}$$

$$t^2+t+s^6+s^2+a_6 = 0 \tag{3.8}$$

식(3.7)은 2개의 해 s_1과 s_1+1을 가진다. $Tr(s_1^6+s_1^2+a_6)=0$ 이므로 다음을 알 수 있다.

$$Tr\left((s_1+1)^6+(s_1+1)^2+a_6\right)=0$$

식 (3.7)과 (3.8)은 4개의 해를 가지고 있으므로 E_2에 동형인 $q^2/4$ 개의 곡선이 있다.

결국 E_3을 다음의 곡선으로 하자.

$$E_3 : y^2+y=x^3+x+1$$

식 (3.3)과 (3.4)가 F_{2^m}상에 해가 없을 검증하여 F_{2^m}상에 $E_1 \ncong E_3$그리고 $E_2 \ncong E_3$임을 쉽게 검사할 수 있다. 전 절에서와 같이 E_3에 동형인 $q^2/4$개의 곡선이 있다는 것을 검증할 수 있다. 따라서 모든 초특이 타원 곡선에 대한 해를 찾을 수 있고 다음과 같이 요약한다.

정리 3.5 *홀수 m에 대하여 F_{2^m} 상에 초 특이 타원 곡선에는 3가지 동형 류가 있다. 각각의 대표 곡선은*

(i) $y^2+y=x^3$

(ii) $y^2+y=x^3+x$

(iii) $y^2+y=x^3+x+1$

제 5 절 짝수 m의 F_{2^m} 상 초특이 타원 곡선의 동형 류

짝수 m이고 F_{2^m} $(q=2^m)$ 상 초특이 타원 곡선의 7가지 동형 류가 있다는 것을 엄밀히 증명한다.

E/F_{2^m}은 다음의 곡선이라 하자.

$$E : y^2 + a_3y = x^3 + a_4x + a_6 \qquad (a_3 \neq 0)$$

다음의 3가지 형태를 고려한다.

Type I: a_3이 3승근이 아님

Type II: a_3이 3승근이고 $Te(a_4) \neq 0$

Type III: a_3이 3승근이고 $Te(a_4) = 0$

Type I 곡선

x의 계수가 0인 Type I의 곡선을 Type Ia라고 부르자. E_1을 Type Ia 곡선이라 하자.

$$E_1 : y^2 + a_3y = x^3 + a_6$$

그리고

$$E_2 : y^2 + \overline{a}_3y = x^3 + \overline{a}_4x + a_6$$

이 F_{2^m}상의 곡선이고 E_1에 동형이라고 하자. F_{2^m}상 $E_1 \cong E_2$이므로 다음의 식을 만족하는 $u_1, s_1, t_1 \in F_{2^m}$이 존재한다.

$$u^3 = a_3/\overline{a}_3 \tag{3.9}$$

$$s^4 + a_3s + u^4\overline{a}_4 = 0 \tag{3.10}$$

$$t^2 + a_3t + s^6 + a_6 + u^6\overline{a}_6 = 0 \tag{3.11}$$

$\overline{a} = a_3/u^3$이고 a_3은 3승근이 아니므로 $\overline{a}_3$도 3승근이 아니다. E_1을 E_2로 변환하는 허용하는 변수 변환의 수를 세어 본다. 이 것은 F_{2^m}에서 식 (3.9), (3.10), (3.11)에서 해 (u, s, t)의 모든 가짓 수를 세면 가능하다.

식 (3.9)는 정확히 3개의 해 u_1, c_1u_1, c_2u_1이 있다. a_3이 3승근이 아니므로 식(3.10)은 u의 각 선택에 대하여 정확히 1개의 해가 있다. $u = u_1, c_1u_1, c_2u_1$에 대하여 식(3.10)에의 유일한 해는 각각 $s = s_1, c_1s_1, c_2s_1$이다. 결국 $(u, s) = (u_1, s_1)$, (c_1u_1, c_1s_2), (c_2u_1, c_2s_1)에 대하여 식(3.11)에는 2개의 해 즉, t_1과 $t_1 + a_3$가 있다. E_1을 E_2로 변환하는 6개의 허용하는 변수 변환이 있다.

허용하는 변수 변환의 총 가짓수가 $(q-1)q^2$이므로 E_1에 동형인 곡선의 수는 $(q-1)q^2/6$이다. E_1을 Type Ia로 변환하는 허용하는 변수 변환은 $(q-1)q$개

가 있다. 이것은 $\overline{a}_4 = (s^4 + a_3 s)/u^4$이므로 $s = 0$ 이어야만 $\overline{a}_4 = 0$이다. E_1 자체를 포함하여 E_1으로 동형인 Type Ia 곡선이 $(q-1)q/6$개가 있다. 총 $2(q-1)q/3$ 개의 Type Ia 곡선이 있으므로, Type Ia 곡선은 4 종류의 동형 류에 분포되어 있을 것이다. 각 동형 류에는 $(q-1)q^2/6$개의 Type I 곡선이 있으며 그 중 $(q-1)q/6$ 개의 Type Ia 곡선이 있다. 이런 4 종류는 $2(q-1)q^2/3$ 개의 Type I 곡선을 망라한다.

Type II 곡선

a_3이 3승근이므로 Type II (그리고 Type III) 곡선은 $y^2+y = x^3+a_4x+a_6$의 형태를 가진다고 가정한다. 허용하는 변수 변환은 $(x, y) \to (u^2x+s^2, u^3y+u^2sx+t)$ 이고 $u, s, t \in F_{2^m}$이고 $u^3 = 1$이다. E_1이 다음과 같이 Type II 의 곡선이라 하자.

$$E_1 : y^2 + y = x^3 + a_4 x,\ Te(a_4) = 1$$

그리고

$$E_2 : y^2 + \overline{a}_3 y = x^3 + \overline{a}_4 x + \overline{a}_6$$

는 E_1 에 동형인 F_{2^m} 상의 임의의 곡선이라고 하자. 그러면 $\overline{a}_3$은 3승근이어야 한다. 그리고 $\overline{a}_3 = 1$이라고 가정한다. $F_{2^m}E_1 \cong E_2$이므로 다음의 방정식을 만족하는 $u_1, s_1, t_1 \in F_{2^m}$이 존재한다.

$$u^3 = a1 \tag{3.12}$$

$$s^4 + s + a_4 + u\overline{a}_4 = 0 \tag{3.13}$$

$$t^2 + a_3 t + s^6 + a_4 s^2 + \overline{a}_6 = 0 \tag{3.14}$$

이다. 그리고

$$\begin{aligned} Te(\overline{a}_4) &= Te(\frac{s^4 + s + a_4}{u}) \\ &= Te(\frac{s^4}{u^4} + Te(\frac{s}{u}) + Te(\frac{a_4}{u}) = Te(\frac{a_4}{u}) \end{aligned}$$

이다.

만일 $u = 1, c_1, c_2$ 이면 각각 $Te(a_4/u) = 1, c_2, c_1$ 이다. 그래서 $Te(\overline{a}_4) \neq 0$이고 E_2도 Type II 곡선이다. E_1에서 E_2로 변환하는 허용하는 변수 변환 가짓수를 세어본다.

$u^3 = 1$이므로 $u = 1, c_1, c_2$이다. 각 u 값에 대하여 각각 $Te(a_4 + u\overline{a}_4) = 0$ 또는 $Te(a_4 + u\overline{a}_4) \neq 0$에 따라 ($F_{2^m}$에서) 식 (3.13)은 4개의 서로 다른 해가 있던

가 해가 없다. $u = 1, c_1, c_2$에 대하여 식(3.13)은 $Te(\overline{a}_4) = 1, c_2, c_1$이어야만 각각 4개의 해를 가지고 있다는 것을 알았다. 일반성을 잃지 않고, $Te(\overline{a}_4) = 1$이라고 가정하자. 그러면 방정식

$$s^4 + s + a_4 + \overline{a}_4 = 0$$

은 4개의 서로 다른 해, $s = s_1, s_1+1, s_1+c_1, s_1+c_2$를 가진다. (s_1, t_1)이 식(3.14)에의 해이므로

$$Tr(s_1^6 + a_4 s_1^2 + \overline{a}_6) = 0$$

이 된다. 그러면

$$\begin{aligned} Tr\left((s_1+1)^6 + a_4(s_1+1)^2 + \overline{a}_6\right) &= Tr(a_4) = 0, \\ Tr\left((s_1+1)^6 + a_4(s_1+c_1)^2 + \overline{a}_6\right) &= Tr(c_2 a_4) = 1, \\ Tr\left((s_1+1)^6 + a_4(s_1+c_2)^2 + \overline{a}_6\right) &= Tr(c_1 a_4) = 1. \end{aligned}$$

식(3.14)는 $s = s_1$ 과 $s = s_1 + 1$일 때에만 해를 가진다. 식 (3.12) - (3.14)에 대하여 4개의 해 (u, s, t)가 있다고 결론을 내린다.

그러면 $3q^2$의 허용하는 변수 변환이 있고 E_1과 동형인 $3q^2/4$개의 Type II 곡선이 있다. Type II 곡선의 총 가짓 수는 $3q^2/4$개 이므로 Type II 곡선은 타원 곡선의 동형 류를 형성한다고 결론 지을 수 있다.

Type III 곡선

E_1은 Type III 곡선으로 다음과 같은 방정식으로 주어진다.

$$E_1 : y^2 + y = x^3$$

그리고

$$E_2 : y^2 + y = x^3 + \overline{a}_4 x + \overline{a}_6$$

라고 하고 E_1에 동형인 F_{2^m}상의 임의의 곡선이라고 하자. F_{2^m}상에 $E_1 \cong E_2$이므로 다음을 만족하는 $u_1, s_1, t_1 \in F_{2^m}$이 있다.

$$u^3 = 1 \tag{3.15}$$

$$s^4 + s + u\overline{a}_4 = 0 \tag{3.16}$$

$$t^2 + t + s^6 + \overline{a}_6 = 0. \tag{3.17}$$

그리고

$$Te(\overline{a}_4) = Te(\frac{s^4+s}{u}) = Te(\frac{s^4}{u^4}) + Te(\frac{s}{u}) = 0$$

을 주의하고 E_2 곡선은 Type III 곡선이 된다. 앞에서와 같이 E_1을 E_2로 변환하는 허용하는 변수 변환의 가짓수를 세어본다.

$u^3 = 1$이므로 $u = 1, c_1, c_2$를 얻는다. $Te(\overline{a}_4) = 0$이므로 $Te(c_1\overline{a}_4) = 0$과 $Te(c_2\overline{a}_4) = 0$을 얻는다. 각 $u = 1, c_1, c_2$에 대하여 식 (3.16)은 F_{2^m}상에 4개의 서로 다른 해를 가진다.

식(3.16)에 12개의 해는 다음과 같다

$$\begin{aligned} u = 1 \quad &; \quad s = s_1, s_1+1, s_1+c_1, s_1+c_2 \\ u = c_1 \quad &; \quad s = c_1s_1, c_1s_1+1, c_1s_1+c_1, c_1s_1+c_2 \\ u = c_2 \quad &; \quad s = c_2s_1, c_2s_1+1, c_2s_1+c_1, c_2s_1+c_2 \end{aligned} \tag{3.18}$$

(s_1, t_1)이 식(3.17)에 해이므로 $Tr(s_1^6 + \overline{a}_6) = 1$을 얻는다. 이 사실을 이용하여 식(3.18)에서 s에 대하여 12개의 각 선택에 대하여 $Tr(s^6 + \overline{a}_6) = 0$을 쉽게 검사할 수 있다. 그래서 식(3.15) -(3.17)은 24개의 해 (u, s, t)가 있다.

$3q^2$개 허용하는 변수 변환이 있으므로 E_1에 동형인 $3q^2/24$개의 Type III 곡선이 있다. 이것은 $q^2/4$개의 Type III 곡선의 반을 망라한다.

E_3를 Type III 곡선으로

$$E_3 : y^2 + y = x^3 + \alpha$$

라 하고 $\alpha \in F_{2^m}, Tr(\alpha) = 1$이라 하자. $E_1 \ncong E_3$이므로 다음의 방정식

$$\begin{aligned} u^3 &= 1 \\ s^4 + s &= 0 \\ t^2 + t + s^6 + \alpha &= 0 \end{aligned}$$

은 F_{2^m}상에서 해 (u, s, t)가 없다. 따라서 나머지 $q^2/4$ 개의 Type III 곡선은 E_1에 동형이 아님을 유도하고 E_3라고 표시하는 동형 류에 속할 것이다. 이 결과를 요약하면 다음과 같다.

정리 3.6 *m이 짝수이고 F_{2^m} 상에 초 특이 타원 곡선은 7개의 동형 류가 있다. γ를 F_{2^m}에 3승근이 아니고 $\alpha, \beta, \delta, \omega \in F_{2^m}$이 있어 $Tr(\gamma^{-2}\alpha) = 1, Tr(\gamma^{-4}\beta) = 1, Te(\delta) \neq 0, Tr(\omega) = 1$이라고 하자. 각 류를 대표하는 곡선은 :*

(i) $E_1 : y^2 + \gamma y = x^3$ *(Type I)*

(ii) $E_2 : y^2 + \gamma y = x^3 + \alpha$ *(Type I)*

(iii) $E_3 : y^2 + \gamma^2 y = x^3$ *(Type I)*

(iv) $E_4 : y^2 + \gamma^2 y = x^3 + \beta$ *(Type I)*

(v) $E_5 : y^2 + y = x^3 + \delta x$ *(Type II)*

(vi) $E_6 : y^2 + y = x^3$ *(Type III)*

(vii) $E_7 : y^2 + y = x^3 + \omega$ *(Type III)*

표(5)에는 각 곡선의 크기와 군 구조와 함께 F_4 상에서 타원 곡선의 13개 동형 류의 대표 곡선을 정리하였다. F_4의 원소를 $0, 1, c_1, c_2$라고 한다.

표 3.2: F_4상 타원 곡선의 13개 동형 류의 대표 곡선

대표 곡선 E	j-불변량	$\#E(F_4)$	군 구조
$y^2 + xy = x^3 + 1$	1	8	Z_8
$y^2 + xy = x^3 + c_1x^2 + 1$	1	2	Z_2
$y^2 + xy = x^3 + c_1$	c_2	4	Z_4
$y^2 + xy = x^3 + c_1x^2 + c_1$	c_2	6	Z_6
$y^2 + xy = x^3 + c_2$	c_1	4	Z_4
$y^2 + xy = x^3 + c_1x^2 + c_2$	c_1	6	Z_6
$y^2 + c_1y = x^3$(Type I)	0	3	Z_3
$y^2 + c_1y = x^3 + 1$(Type I)	0	7	Z_7
$y^2 + c_2y = x^3$(Type I)	0	3	Z_3
$y^2 + c_2y = x^3 + 1$(Type I)	0	7	Z_7
$y^2 + y = x^3 + x$(Type II)	0	5	Z_5
$y^2 + y = x^3$(Type III)	0	9	$Z_3 \oplus Z_3$
$y^2 + y = x^3 + c_1$(Type III)	0	1	Z_1

제 6 절 점의 수

F_{2^m}상에 초특이 곡선, E에 대한 $\#E(F_{2^m})$을 결정하자. 이런 곡선의 군 구조는 보조정리 (2.2)에 의하여 결정된다.

(i) 홀수 m

이 경우 F_{2^m}상 초특이 곡선의 3개 동형 류의 각각은 F_2에서 계수를 대표로 가지고 있다. Weil 정리를 이용하여 F_{2^m}상 곡선의 위수를 쉽게 결정할 수 있다. 결과는 표 (6)에 정리하였다. (표 중에 k값은 추후에 기술한다.)

표 3.3: m이 홀수인 때, F_{2^m}상 초특이 곡선의 위수

곡선 E	m	$\#E(F_{2^m})$	군 형태	k
$y^2+y=x^3$	홀수	$q+1$	순환 군	2
$y^2+y=x^3+x$	$m \equiv 1,7 \pmod 8$	$q+1+\sqrt{2q}$	순환 군	4
	$m \equiv 3,5 \pmod 8$	$q+1-\sqrt{2q}$	순환 군	4
$y^2+y=x^3+x+1$	$m \equiv 1,7 \pmod 8$	$q+1-\sqrt{2q}$	순환 군	4
	$m \equiv 3,5 \pmod 8$	$q+1+\sqrt{2q}$	순환 군	4

(ii) 짝수 m

$1 \le i \le 7$에 대하여 $\#E_i = \#E_i(F_{2^m}) = q+1-t_i$ 단, $q = 2^m$ 라 하자. 곡선들은 정리 (3.6)에 정의된 것들이다. 정리 (3.2)에 의하여 t_i의 7가지 값은 $0, 2\sqrt{q}, -2\sqrt{q}, \sqrt{q}, \sqrt{q}, -\sqrt{q}, -\sqrt{q}$ (반드시 이런 순서는 아니다.) 이다.

우선 $\#E_1 + \#E_2 = 2q+2$ 이고 $t_1 = -t_2$ 인 때를 고찰한다. 이것은 각 $x \in F_q$에서 $Tr(\gamma^{-2}x^3) = 0$ 또는 $Tr(\gamma^{-2}x^3 + \gamma^{-2}\alpha)-)$ 이거나 둘 다 그렇지 아니한 때 성립한다. 곡선 E_1, E_2는 타원 곡선의 twisted pair의 한가지 예이다. E_3, E_4와 E_6, E_7는 twisted pair이고 결국 $t_3 = -t_4, t_6 = -t_7$이다. 그리고 $t_5 = 0$이다.

E_6의 계수는 F_2에 있으므로 $\#E_6$를 결정하는 데 Weil 정리를 적용한다. 그리고 $\#E_7$도 적용해 본다. $m \equiv 02 \pmod 4$에 따라 각각 $t_6 = 2\sqrt{q} - 2\sqrt{q}$를 찾는다.

그리고 $t_1, t_3 = \sqrt{q} - \sqrt{q}$을 안다. 그것의 정확한 값을 다음과 같이 결정한다. $\gamma = g^{-1}$라 하고, g는 F_{2^m}는 생성원이다. 그리고 다음 집합을 생각한다.

$$\begin{aligned} A = \{x^3 : x \in F_{2^m}\} &= \{g^{3i} : 1 \le i \le (2^m-1)/3\} \cup \{0\}, \\ B = \{\gamma^{-2}x^3 : x \in F_{2^m}\} &= \{g^{3i+2} : 1 \le i \le (2^m-1)/3\} \cup \{0\}, \\ C = \{\gamma^{-4}x^3 : x \in F_{2^m}\} &= \{g^{3i+1} : 1 \le i \le (2^m-1)/3\} \cup \{0\}, \end{aligned}$$

$(A\backslash\{0\}, B\backslash\{0\}, C\backslash\{0\})$는 $F_{2^m}^*$의 부분이므로 trace가 0인 F_{2^m}의 원소는 정확히 반이 있으므로 다음을 유도한다.

$$\#E_1 + \#E_3 + \#E_6 = 3q + 3$$

그리고 $t_1 + t_3 = -t_6$이다.

만일 $m \equiv 0 \pmod 4$이면 $t_1 = t_3 = -\sqrt{q}$을 가질 것이고, 만일 $m \equiv 2 \pmod 4$이면 $t_1 = t_3 = \sqrt{q}$을 가질 것이다. 곡선 E_i, $1 \le i \le 7$의 위수는 표 (6)에 나열하였다. $E_1 : y^2 + \gamma y = x^3$과 $E_2 : y^2 + \gamma^2 y = x^3$은 타원 곡선으로서는 동형이 아니나, $E_1(F_q)$와 $E_3(F_q)$는 동형이다.

표 3.4: m이 짝수일 때, F_{2^m} 상 초 특이 곡선의 위수

곡선 E_i	m	$\#E_i(F_{2^m})$	군 형태	k
$y^2 + \gamma y = x^3$	$m \equiv 0 \pmod 4$	$q + 1 + \sqrt{q}$	순환군	3
	$m \equiv 2 \pmod 4$	$q + 1 - \sqrt{q}$	순환군	3
$y^2 + \gamma y = x^3 + \alpha$	$m \equiv 0 \pmod 4$	$q + 1 - \sqrt{q}$	순환군	3
	$m \equiv 2 \pmod 4$	$q + 1 + \sqrt{q}$	순환군	3
$y^2 + \gamma^2 y = x^3$	$m \equiv 0 \pmod 4$	$q + 1 + \sqrt{q}$	순환군	3
	$m \equiv 2 \pmod 4$	$q + 1 - \sqrt{q}$	순환군	3
$y^2 + \gamma y = x^3 + \beta$	$m \equiv 0 \pmod 4$	$q + 1 - \sqrt{q}$	순환군	3
	$m \equiv 2 \pmod 4$	$q + 1 + \sqrt{q}$	순환군	3
$y^2 + y = x^3 + \delta x$	m 짝수	$q + 1$	순환군	2
$y^2 + y = x^3$	$m \equiv 0 \pmod 4$	$q + 1 - 2\sqrt{q}$	$Z_{\sqrt{q}-1} \oplus Z_{\sqrt{q}-1}$	1
	$m \equiv 2 \pmod 4$	$q + 1 + 2\sqrt{q}$	$Z_{\sqrt{q}+1} \oplus Z_{\sqrt{q}+1}$	1
$y^2 + y = x^3 + \omega$	$m \equiv 0 \pmod 4$	$q + 1 + 2\sqrt{q}$	$Z_{\sqrt{q}+1} \oplus Z_{\sqrt{q}+1}$	1
	$m \equiv 2 \pmod 4$	$q + 1 - 2\sqrt{q}$	$Z_{\sqrt{q}-1} \oplus Z_{\sqrt{q}-1}$	1

F_{2^m}상 임의의 초특이 타원 곡선 E가 주어지면, 우선 어떤 동형 류에 속하는가에 따라 $\#E(F_{2^m})$을 계산할 수 있다. 이것은 정리 (2.2)에 주어진 적절한 근 탐색 문제를 해결하면 얻을 수 있다. F_{2^m}상에 다항식의 근을 구하는 몇가지 효율적인 알고리즘이 있다. 예를들면 [10]을 참조한다.

제 7 절 참조 사항

Waterhouse의 연구는 Deuring의 논문[32]에 근거로 하고 있다. Deuring은 F_q상에 정의된 2개의 타원 곡선이 그들이 동형이면 F_q에 동형일 것이리고 생각하였다. Waterhouse의 몇가지 연구는 Rück에 의하여 유한체 상에 genus 2의 대수곡선의 Jacobian으로 일반화하였다.

3절에서 6절까지의 내용은 [94]에서 인용하였다.

제 4 장

이산 대수 문제

어떤 군 G 상에서 이산 대수 문제의 어려움에 군거를 둔 많은 공개키 암호시스템이 있다. 최근에 이산 대수 문제는 많은 주목을 받았고, 여러가지 기법을 이용한 수 많은 알고리즘이 제시되었다. 1절에서는 이 문제를 해결하기 위한 알고리즘을 조사하고 2절에서는 특이 타원 곡선과 어떤 군 상의 이산 대수 문제를 유한체 상의 이산 대수 문제로 축약하는 방법을 공부한다.

제 1 절 알고리즘

G가 위수 n의 유한 (곱셈) 순환 군이라고 하고, α를 G의 생성원이라고 하자.

기저 α인 β의 이산 대수는 $\log_\alpha \beta$로 표기하고, $\beta = \alpha^x$가 되도록 하는 유일한 정수 $x, 0 \leq x < n$이다. α를 계속하여 멱승을 하여 β가 되도록 하는 알고리즘이 명백히 성립하나, $O(n)$의 군 연산이 필요하므로 n이 클 경우에는 불충분하다.

대수를 찾는 알고리즘은 다음과 같이 분류할 수 있다.

(i) 임의의 군에서 동작하는 알고리즘 (Square root 방법)

(ii) 임의의 군에서 동작하나 준군(subgroup)의 구조를 이용하는 방법 (Pohlig-Hellman 방법)

(iii) Index calculus 방법

(iv) 군 사이의 동형 사상을 이용하는 방법

1.1 Square root 방법

$m = \lceil \sqrt{n} \rceil$라고 하자.

Baby-Step Giant-Step Method

$x = \log_\alpha \beta$이면 $x = jm + i$ (단, $1 \le i < m$) 로 표기 할 수 있다. $0 \le i < m$에서 쌍 (i, α^i)를 계산하고 2번째 값으로 표에 나열한다. $j(0 \le j < m)$에 대하여 $\beta\alpha^{-jm}$를 계산하고 이 값이 표 상 2번째 값과 일치하는 지를 조사한다. 어떤 i, $0 \le i < m$ 에 대하여 만일 $\beta\alpha^{-jm} = \alpha^i$이면, $\beta = \alpha^{i+jm}$이므로 $\log_\alpha \beta = i + jm$이다.

이 알고리즘은 표에 $O(m)$개 값을 필요로 한다. 표를 정렬하고 각 j 값에 대한 탐색하는 데, 총 $O(m \log m)$의 연산을 필요로 한다 (연산이라고 하면 군상의 연산 또는 비교를 의미한다.). 10^{40}개 요소를 갖는 군은 현재의 기술로 이 공격이 불가능하게 한다.

Pollard ρ Method

Pollard[123]는 대수 문제를 확률적으로 찾는 방법을 제시하였는 데 사전에 표 계산의 필요성을 없앴다.

군 G를 거의 균등한 크기인 3개의 집합 S_1, S_2, S_3으로 구분한다. (예를들면 $1 \notin S_2$ 되도록 주의하여야 한다.) $x_0 = 1$로 하고 군의 요소 $x_0, x_1, x_2, \ldots$의 수열을 $x_0 = 1$로 하고 $i \ge 1$에 대하여 다음과 같이 정의한다.

$$x_i = \begin{cases} \beta x_{i-1}, & x_{i-1} \in S_1 \\ x_{i-1}^2, & x_{i-1} \in S_2 \\ \alpha x_{i-1}, & x_{i-1} \in S_3 \end{cases}$$

x_{i-1}의 값을 가진 집합 S_1, S_2, S_3에 따라 $a_0 = b_0 = 0$이고 $a_{i+1} \equiv a_i + 1, 2a_i, a_i \pmod n$과 $b_{i+1} \equiv b_i + 1, 2b_i, b_i \pmod n$로 하는 정수 수열 $\{a_i\}, \{b_i\}$인 것을 정의하면 쉽게 군 요소를 생성할 수 있다. Floyd의 주기 탐색 알고리즘을 이용하면 Pollard는 6개 값 $(x_i, a_i, b_i, x_{2i}, a_{2i}, b_{2i})$를 $i = 1, 2, \ldots$에 $x_i = x_{2i}$가 되도록 찾는다. 이 단계에서

$$\beta^r = \alpha^s$$

을 구한다. 단, $r \equiv a_i - a_{2i}$, $s \equiv b_{2i} - b_i \pmod n$이다. 이것으로

$$r \log_\alpha \beta \equiv s \pmod n$$

을 얻는다. $\log_\alpha \beta$에 대한 $d = \gcd(r, n)$개의 가능한 값이 있다. 만일 d가 작으면 각각의 가능성에 대하여 옳바른 값을 찾아 낼 수 있다.

만일 G의 랜덤 수열의 요소처럼 $\{x_i\}$가 행동하는 가정을 한다면 이 방법의 기대되는 소요 시간은 $O(m)$의 군 연산이다. 만일 G의 위수가 10^{40} 이상이면 이 방법은 불가능하다.

1.2 Pohlig-Hellman 방법

순환 군[122]에서 대수를 계산하는 방법은 군의 위수를 소인수 분해하는 방법을 이용하자.

$$n = \prod_{i=1}^{t} p_i^{\lambda_i}$$

로 하고 p_i는 소수, λ_i는 각 $1 \le i \le t$에 양의 정수이다. 만일 $x = \log_\alpha \beta$라 하면 각각의 $i, 1 \le i \le t$에 대하여 $x \bmod p_i^{\lambda_i}$를 Chinese Remainder Theorem를 이용하여 $x \bmod n$을 계산할 수 있다. 우선 $z \equiv x \pmod{p_1^{\lambda_1}}$으로 시작하자.

$0 \le z_i \le p_1 - 1$에 대하여

$$z = \sum_{i=0}^{\lambda_1 - 1} z_i p_1^i$$

를 가정하자.

$\gamma = \alpha^{n/p_1}$는 G 상에서 p_1차 단위 군 (root of unity)이라 하자. 그러면 square root 방법을 이용하여 G에서 위수 p_1의 순환군에서 기저 γ로 하는 γ^{z_0}의 대수를 결정할 수 있다. 이로서 z_0를 계산한다. 만일 $\gamma_1 > 1$이면 z_1을 계산하고

$$(\beta\alpha^{-z_0})^{n/p_1^2} = (\alpha^{\sum_{i=1}^{\lambda_1 - 1} z_i p_1^i})^{n/p_1^2} = \gamma^{z_1}$$

마찬가지로 z_1은 square root 방법에 의하여 계산한다. 유사하게 $0 \le i < \lambda_1$에 대한 모든 z_i를 계산하여 $x \bmod p_1^{\lambda_1}$을 구한다.

이 기법은 $O(\sum_{i=1}^{t} \lambda_i (\log n + \sqrt{p_i} \log p_i))$ 군 연산이 필요하고 [122] 위수가 smooth integer이면 (즉, n이 작은 소수로만 나누어 진다.) 효과적이다.

1.3 Index Calculus 방법

복잡도 이론에 의하면 subexponential 알고리즘이란 다음과 같은 수행 시간이 필요한 것이다.

$$L[x, c, \alpha] = O(\exp((c + o(1))(\ln x)^\alpha (\ln \ln x)^{1-\alpha})) \tag{4.1}$$

여기서 x는 입력 공간의 크기이고 c는 상수이고 $0 < \alpha < 1$이다. subexponential 알고리즘은 입력 크기에 exponential(polynomial) 알고리즘에 비하여 점근적으로 빠르다 (느리다). 식(4.1)에서 $\alpha = 0$이면 $\ln x$에 대하여 다항식이 되고, $\alpha = 1$이면 $\ln x$에 대하여 exponential 시간이 된다.

확률적 준 다항식 (subexponential) 시간 알고리즘이란 랜덤 알고리즘으로 기대되는 수행 시간이 입력 크기의 준 다항식 (subexponential) 로 제한되어 있다는 것을 의미한다.

Index calculus 방법의 첫번째 단계로 고정된 부분 집합 즉, factor base라고 하는 $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_t\}$의 요소에 대한 대수 문제를 구하는 것이다. 랜덤 수 s를 뽑아, α^s를 Γ상의 요소의 곱으로 표현해 보자.

$$\alpha^s = \prod_{i=1}^{t} \gamma^{a_i} \tag{4.2}$$

만약 성공하면 식(4.2)의 양변에 대수를 취하면 선형 congruence 방정식을 얻는다.

$$s \equiv \sum_{i=1}^{t} a_i \log_\alpha \gamma_i \pmod{n} \tag{4.3}$$

식(4.3)과 같은 형태의 관계를 충분히 모은 후에 희망적으로 미지수 $\log_\alpha \gamma_i, 1 \leq i \leq t$를 계산할 수 있다.

2번째 단계로 $\log_\alpha \beta$를 다음과 같이 구한다. 반복적으로 정수 s를 $\alpha^s\beta$가 Γ상의 요소로

$$\alpha^s\beta = \prod_{i=1}^{t} \gamma_i^{b_i} \tag{4.4}$$

가 되도록 선택한다.

양변에 대수를 취하면

$$\log_\alpha \beta = \sum_{i=1}^{t} b_i \log_\alpha \gamma_i - s \pmod{n} \tag{4.5}$$

를 얻는다. Index calculus 방법의 기술을 마치려면 factor base Γ를 적절히 선택하는 방법과 식(4.2)과 식(4.4)의 관계를 효과적으로 발생하는 방법이 필요하다. 적절한 Γ라 함은 집합의 수가 작고 (1단계에서 방정식이 너무 많지 아니할 것) 동시에 G의 요소가 Γ에 많을 것 (식(4.2)와 식(4.4)의 관계를 시도하는 데 시도 횟수가 많지 아니할 것)을 의미한다.

p가 소수인 체 F_p에서 Γ는 우선 t개의 소수를 선택한다. 식(4.2)의 관계를 발생하기 위하여 α^s를 구간 $[1, p-1]$에의 정수로 표현하고 trial division에 의하여 Γ상에 α^s의 소인수 분해를 시도한다. 적절히 t를 선택하면 Index calculus 방법의 기대 소요 시간은 $L[p, 2, 1/2]$이다. F_p의 현실적인 결과로 수행시간이 $L[p, 1, 1/2]$인 Gauss 정수법[30]이 있다. 현실적이지는 아니하지만 F_p에 가장 빠른 방법으로 수행시간이 $L[p, 3^{2/3}, 1/3]$인 수체 선별법[50]이 있다.

유한체 F_{2^m} (또는, 일반적으로 p가 고정된 F_{p^m}) 에서 F_{2^m}의 요소를 m-1 차 다항식으로 $F_2[x]$의 다항식으로 표현할 수 있다. 곱셈은 $F_2[x]$상에 고정된 기약 다항식으로 modulo를 취하여 연산이 가능하다. 집합 Γ는 임의의 한계로 최대 b 차의 모든 기약 다항식의 집합으로 취한다. 식(4.2)의 관계를 구하기 위하여 α^s를 최대 $m-1$차의 다항식으로 표현하고 Γ에 있는 다항식의 곱으로 $F_2[x]$상에서 소인수 분해한다. 이 방법의 수행 시간은 (약간의 향상 후) $L[2^m, c, 1/3]$이고 $1.3507 \leq c \leq 1.4047$이다.

F_p와 F_{2^m}에서 언급한 알고리즘은 모두 확률적이고 수행시간은 엄밀하게 증명이 되지 아니한 경험적인 사실에 의존한다. F_p와 F_{2^m} 상의 최량의 알고리즘은 Pomerance[124]에 의하여 엄격하게 증명되었으며, 기대되는 수행 시간은 각각 $L[p, \sqrt{2}, 1/2]$, $L[2^m, \sqrt{2}, 1/2]$ 이다.

m이 고정된 체 F_{p^m}에 대하여는 수체 선별법[51]이 가장 좋은 알고리즘으로 경험적인 수행 시간은 $L[p^m, c, 1/3]$ (단,c는 m에 의존하는 상수) 이다. $\log p < m^{0.98}$인 값에서 F_{p^2}와 F_{p^m}에 엄밀히 증명된 알고리즘은 Lovoron[84]에 의하면 수행시간이 $L[p^m, c, 1/2]$ (단 c는 양의 어떤 수)이다.

1.4 타원곡선 상의 Index Calculus 방법

Miller[100]는 타원 곡선 군에서의 Index calculus 방법을 토의하였는 데, F_q^*와 달리 factor base Γ가 아주 자연적인 (작은 크기의 소수, 작은 차수의 기약 다항식) 후보가 $E(F_q)$ 상에는 없을 것 같다고 하였다. 가장 자연스로운 것은 Q가 유리수의 체이면 $E(Q)$ 상에 height가 낮은 점들이다. (점의 height는 그 점을 표현하는 데 필요한 비트의 수를 의미한다.) 그러나, $E(Q)$ 상에는 작은 height의 점들이 거이 없을 것이라고 주장하였다. 더욱이, 그러한 Γ가 존재한다 하더라도 $E(F_q)$ 상의 점을 $E(Q)$로 lifting하는 효율적인 알고리즘을 찾는 것은 절망적이다.

제 2 절 어떤 대수 문제를 유한체로의 축소

동일한 위수를 가진 2개의 순환군은 동형일 지라도 한 곳에서 대수문제를 효과적으로 푼다고 하여 다른 한 쪽에서 반드시 효율적이라고 할 수 없다. 위수 n을 가진 임의의 순환 군이 덧셈 군 Z_n과 동형이라면 Z_n에서의 대수 계산은 확장 유크리드 알고리즘을 이용하면 쉽게 해결 된다는 것은 자명하다. 결국, 이산 대수 문제는 다음과 같이 재 정의를 할 수 있다. 위수 n을 가진 순한 군과 Z_n 덧셈 순환 군간의 동형 사상을 계산적으로 효과적인 알고리즘을 찾는 것이다.

여기서는 어떤 군에서 대수 문제를 어떤 유한 체 상의 대수 문제로 (다항식 또는 확률적 다항식 시간에) 축소하는 것을 연구한다. F_q 상에 정의된 특이 타원 곡선 E의 대수 문제는 F_{q^k} (단, $k = 1, 2$이고 E가 node를 가지고 있을 때) 상의 대수 문제보다 어렵지 않다. 만일 E가 cusp이면 대수 문제는 쉽게 계산된다. 또한, F_q 상에 Pell 방정식으로 정의된 genus 0 인 타원 곡선 류의 대수 문제는 F_{q^k} (단, $k = 1, 2$) 상의 대수 문제보다 어렵지 않다.

이 결과들은 이런 군에서의 군 연산이 F_q 상에서의 곱셈 연산 보다 복잡하므로 처음에는 놀라운 것일 수도 있다. 이런 군에서의 군 연산은 F_{q^k} 상의 군 연산보다 더욱 비싸기 때문에, 앞에서의 군들은 이산 대수 문제의 어려움에 안전성을 둔 암호 프로토콜을 구현하는 데는 아무런 이점이 없다고 결론 지울 수 있다.

2.1 특이 타원 곡선

E는 체 F 상에서 정의된 특이 타원 곡선이라고 하자. 즉, E는 다음의 특이 Weierstrasss 방정식으로 주어진다.

$$f(x, y) \;=\; y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \tag{4.6}$$

그러면, E는 정확히 하나의 특이점을 가지고 이 점이 $P = (x_0, y_0) \in E(K)$ 라고 가정한다. 변수 변환 $x \to x' + x_0$, $y \to y' + y_0$로 하고, 특이점을 $P = (0, 0)$이라고 가정한다. $f(P) = 0, \frac{\delta f}{\delta x}(P) = 0, \frac{\delta f}{\delta y}(P) = 0$ 이므로 $a_6 = a_4 = a_3 = 0$이고 Weierstrass 방정식은 다음과 같이 간단히 된다.

$$E : y^2 + a_1xy - x^3 - a_2x^2 = 0, \qquad a_1, a_2 \in K \tag{4.7}$$

$y^2 + a_1xy - a2x^2 = (y - \alpha x)(y - \beta x)$라고 하고 $\alpha, \beta \in K$ 또는 (K의 quadratic extension인) K_1 이다. 그러면 P는 만일 $\alpha \neq \beta$이면 node라고 부르고 $\alpha = \beta$이

면 cusp 라고 부른다. $E_{ns}(K)$를 점 P를 제외하고 무한 원점을 포함한 $(x, y) \in K \times K$의 해 집합으로 한다. $E_{ns}(K)$는 $E(K)$의 non-singular 부분이라고 부른다. 우리는 $E_{ns}(K)$ 상의 덧셈을 tangent-and-chord 법칙을 정의할 수 있다. 다음 결과는 $E_{ns}(K)$가 군이고 군의 구조를 정의한다. 여기서 K^*는 K 영이 아닌 요소들의 곱셈 군을 의미하고, K^+는 K의 덧셈 군을 의미한다.

정리 4.1 *E는 특이점 P를 가진 유한 체 K상에 정의된 특이 타원 곡선이라 한다.*

(i) 만일 P가 node이고, $\alpha, \beta \in K$이면 다음으로 정의된 사상 $\phi : E_{ns}(K) \to K^*$은

$$\phi : \mathcal{O} \mapsto 1 \qquad \phi : (x, y) \mapsto (y - \beta x)/(y - \alpha x)$$

군 동형이 된다.

(ii) 만일 P가 node이고, $\alpha, \beta \notin K_1$이면 L이 norm 1인 요소를 구성하는 K_1^*의 부분 군이라 한다. 다음으로 정의된 사상 $\phi : E_{ns}(K) \to L$은

$$\psi : \mathcal{O} \mapsto 1 \qquad \psi : (x, y) \mapsto (y - \beta x)/(y - \alpha x)$$

군 동형이 된다.

(iii) 만일 P가 cusp이고 다음으로 정의된 사상 $\omega : E_{ns}(K) \mapsto K^+$는

$$\omega : \mathcal{O} \mapsto 0 \qquad \omega : (x, y) \mapsto x/(y - \alpha x)$$

군 동형이 된다.

위의 결과를 이용하면 다음을 얻을 수가 있다.

정리 4.2 *E는 특이점 P를 가진 유한체 F_q 상에 정의된 특이 타원 곡선이라 하자.*

(i) 만일 P가 node이면, $E_{ns}(F_q)$상의 대수 문제는 $\alpha \in F_q$ 또는 $\alpha \notin F_q$에 따라 각각 F_q 또는 F_{q^2} 상의 대수 문제로 다항식 시간으로 축소(reducible) 된다.

(ii) 만일 P가 cusp 이면, $E_{ns}(F_q)$에의 대수 문제는 F_q^+ 상의 대수 문제로 다항식 시간으로 축소된다.

p가 F_q의 표수이고 $q = p^m$이라면

$$F_q^+ \cong \underbrace{F_p^+ \oplus \cdots F_p^+}_{m}$$

이다. F_p^+ 상의 대수 문제는 확장 유크리드 알고리즘에 의하여 다항식 시간내에 효과적으로 풀 수 있음에 주의한다. 따라서 만일 F_p 상에 F_q의 기저가 주어진다면 F_q^+에서 대수 문제는 다항식 시간으로 풀 수 있다

정리 4.3 *E가 cusp를 가진 F_q상에 정의된 타원 곡선이라면 $E_{ns}(F_q)$상의 대수 문제는 다항식 시간으로 풀 수 있다.*

2.2 종수 0의 또 다른 류

Jeff Shallit[139]에 의해 지적된 타원 곡선을 기술한다.

q를 odd prime power라고 하고 D를 F_q의 non-zero element라고 한다. C는 다음의 Pell 방정식에 $(x, y) \in F_q \times F_q$의 해 집합이라고 한다.

$$x^2 - Dy^2 = 1 \tag{4.8}$$

C의 원소를 식(4.8)에 의해 정의되는 genus 0의 대수 곡선의 아핀 점이라고 하자. 연산 $\oplus$는 C 상에 다음과 같이 정의한다. 만일 $(x_1, y_1), (x_2, y_2) \in C$이면,

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1).$$

보조정리 4.1 *$(C, \oplus)$는 아벨 군이다.*

Proof: 덧셈 연산은 닫혀있고, 결합 법칙과 교환 법칙이 성립한다. 항등원은 (1,0)이고 (x, y)의 역은 $(x, -y)$이다. □

$\chi(a)$는 $a \in F_q$ 의 quadaric characteristic이라고 한다. 즉.

$$\chi(a) = \begin{cases} 0, & \text{if } a = 0 \\ 1, & \text{if } a \text{ is a quadratic residue in } F_q \\ -1, & \text{if } a \text{ is a quadratic non-residue in } F_q \end{cases}$$

$\chi(a) = a^{(q-1)/2}$ 임은 널리 알려져 있다. 다음은 C의 군 성질을 결정한다.

정리 4.4 *$(C, \oplus)$ 는 위수 $q - \chi(D)$를 가진 순환 군이다.*

Proof: Case(i) $(\chi(D) = -1)$: $f(W) = W^2 - D \in F_q[W]$로 하자. 그러면 $f(W)$는 F_q 상에 irreducible이다. 그리고, $F_{q^2} \cong F_q[W]/(f(W))$이고 $(F(W))$는 $f(W)$에 의해 생성된 $F_q[W]$의 ideal이다. H를 위수 $q+1$의 F_{q^2}의 유일한 곱셉 부분 군이라고 표기한다. $\alpha = x + yW$는 F_{q^2} 상의 임의의 원소라 하자. 그러면, $\alpha^{q+1} = 1$이어야만 $\alpha \in H$이다.

$$\begin{aligned} \alpha^{q+1} &= (x + yW)^q (x + yW) \\ &= (x + yW^q)(x + yW). \end{aligned}$$

$$W^q = W(W^2)^{(q-1)/2} = WD^{(q-1)/2} = -W$$

이므로

$$\begin{aligned} \alpha^{q+1} &= (x - yW)(x + yW) \\ &= x^2 - y^2 W^2 \\ &= x^2 - Dy^2 \end{aligned}$$

를 갖는다. 결국,$(x, y) \in C$이어야 만 $\alpha \in H$가 성립한다. 따라서, 다음으로 정의된 사상 $\phi : C \to H$는

$$\phi : (x, y) \mapsto x + yW$$

는 전단사 사상이다. 그리고 ϕ가 군 준 동형 사상 (homomorphism)이라는 것은 쉽게 검증된다. H는 위수 $q + 1$의 순환 군이다.
Case(ii) $(\chi(D) = 1)$: $\alpha \in F_q$가 D의 2승근이라 한다. 식(4.8)은 $(x-ay)(x+ay) = 1$로 쓸 수 있다. $u = x - ay$ 그리고 $v = x + ay$라고 하면

$$x = \frac{u + v}{2} \text{ and } y = \frac{v - u}{2a}$$

를 얻는다. 이것은 식(4.8)의 (x, y)와 $uv = 1$의 해 (u, v)를 1-1 대응시킨다. 방정식 $uv = 1$은 $F_q \times F_q$ 에서 정확히 $q - 1$개의 해 (u, v), 즉, 각 $u \in F_q^*$에 대하여 유일한 해를 갖는다. 따라서 다음으로 정의된 사상 $\psi : C \to F_q^*$는

$$\phi : (x, y) \mapsto x - ay$$

는 전단사이다. 또한 ϕ도 군 준 동형 사상임을 쉽게 검증된다. 따라서, C는 위수 $q - 1$인 순환 군을 형성한다. □

만일 $\chi(D) = -1$ 이면, 동형사상 ϕ는 쉽게 계산된다. 반면 $\chi(D) = 1$이면 동형 사상 ψ는 F_q 상에 D의 2승 근이 주어지면 쉽게 계산된다. F_q 상의 2승 근은 확률적 다항식 시간으로 계산되므로[10] 다음의 결과를 얻는다.

정리 4.5 *만일 $\chi(D) = -1$ 이면 C 상의 대수 문제는 F_{q^2} 상의 대수 문제로 일정 시간에 축소된다. 만일 $\chi(D) = 1$ 이면 C 상의 대수 문제는 F_q 상의 대수 문제로 확률적 다항식 시간으로 축소된다.*

제 3 절 참조 사항

이산 대수 문제에 대한 최근의 조사 결과는 McCurley[87]의 기사를 참조하고 Odlyzko[115]는 표수가 2인 유한체에서 대수 문제를 푸는 것에 대한 종합적인 결과를 제시하였다.

genus 0인 임의의 smooth curve는 projective line에 동형이라는 것이 널리 알려져 있다. 여기서 genus 0인 곡선을 제시한 것은 동형 사상을 쉽게 계산할 수 있기 때문이다.

제 5 장

타원 곡선 상 대수 문제

본 장에는 Weil paring을 소개하고, 이것의 효율적인 계산 알고리즘인 Miller 방식을 소개한다. Weil pairing을 이용하여 타원 곡선 상 대수 문제를 유한체 상의 대수 문제로 축소한다. 축소에 따른 암호학적 의미를 고찰하고, Weil pairing을 타원 곡선 군의 type를 결정하는 데 이용한다.

제 1 절 Weil pairing

타원곡선 E를 characteristic p인 유한체 $K = F_q$상에 정의한다.

$D = \sum n_P(P) \in \mathbf{D}$는 인수(divisor)이고, $f \in \overline{K}(E)^*$는 D와 $\mathrm{div}(f)$ 가 disjoint support를 갖도록 하는 유리함수라고 한다. 그러면, D에 정의된 f를 다음과 같이 정의한다.

$$f(D) = \prod_{P \in supp(D)} f(P)^{n_P}$$

1.1 정의

m을 p와 서소 소인 양의 정수라고 하고, $\mu_m \subset \overline{K}^*$을 $m\text{-}th$ roots of unity의 군이라고 하자.

$P, Q \in E[m]$이고 A와 B는 차수 0의 인수로 $A \sim (P) - (\mathcal{O})$, $B \sim (Q) - (\mathcal{O})$이고 A, B는 disjoint support를 가지고 있다고 한다. $f_A, f_B \in \overline{K}(E)$를

$$\mathrm{div}(f_A) = mA, \mathrm{div}(f_B) = mB$$

로 한다.

P와 Q가 모두 m-torsion point 이면 f_A와 f_B는 존재한다. div(f_A)와 B는 disjoint support이고 div(f_B)와 A도 마찬가지이다.

Weil pairing, e_m은 다음의 함수이다.

$$e_m : E[m] \times E[m] \to \mu_m$$

로 다음과 같이 정의된다.

$$e_m(P,Q) = \ f_A(B)/f_B(A).$$

$e_m(P,Q)$의 값은 A, B, f_A, f_B의 선택에 무관하다.

Weil pairing[140]에 대한 유용한 성질을 기술한다.

(i) *Identity :* 모든 $P \in E[m]$에서, $e_m(P,P) = 1$이다.

(ii) *Alternation :* 모든 $P, Q \in E[m]$에서 $e_m(P,Q) = e_m(Q,P)^{-1}$ 이다.

(iii) *Bilinearity :* 모든 $P, Q, R \in E[m]$에 대하여 $e_m(P+Q,R) = e_m(P,R)e_m(Q,R)$이고 $e_m(P,Q+R) = e_m(P,Q)e_m(P,R)$이다.

(iv) *Non-degeneracy :* 만일 $P \in E[m]$ 이면 $e_m(P,\mathcal{O}) = 1$이다. 더욱이, 모든 $Q \in E[m]$에 대하여 만일 $e_m(P,Q) = 1$ 이면 $P = \mathcal{O}$이다.

(v) 만일 $E[m] \subseteq E(K)$이면 모든 $P, Q \in E[m]$ (즉, $\mu_m \subseteq K^*$) 에 대하여 $e_m(P,Q) \in K$이다.

(vi) *Compatible :* 만일 $P \in E[m], Q \in E[mm']$이면, $e_{mm'}(P,Q) = e_m(P,m'Q)$이다.

1.2 주 인수의 함수 계산

유일한 $P \in E$이고 어떤 $f \in \overline{K}(E)$에 대하여 차수 0의 인수 $D \in D^0$는 다음과 같이 쓸 수 있다.

$$D = (P) - (\mathcal{O}) + \mathrm{div}(f) \tag{5.1}$$

f는 $\overline{K}$의 non-zero element에 의한 곱셈으로 결정된다.

canonical form으로 주어지는 2개의 인수를 더하는 방법을 제시하고 결과를 canonical form으로 표현하자.

D_1과 D_2가 차수 0의 인수라고 하자. 여기서

$$D_1 = (P_1) - (\mathcal{O}) + \mathrm{div}(f_1), D_2 = (P_2) - (\mathcal{O}) + \mathrm{div}(f_2),$$

이고 $P_1, P_2 \in E$이고 $f_1, f_2 \in \overline{K}(E)$이다. 또한, $D_1 \notin D_l$이고 $D_2 \notin D_l$ (즉, $P_1 \neq \mathcal{O}, P_2 \neq \mathcal{O}$)이라고 가정한다.

$$D_1 + D_2 = (P_3) - (\mathcal{O}) + \mathrm{div}(f_1 f_2 f_3)$$

이고, $P_3 = P_1 + P_2$, $f_3 = l/v$이고 l은 P_1과 P_2를 지나는 직선의 방정식이고, v는 P_3을 지나는 수직 선분의 방정식이다. (만일 $P_3 = \mathcal{O}$이면, $v = 1$로 놓는다.) 이것은 $\mathrm{div}(f_1 f_2 f_3) = \mathrm{div}(f_1) + \mathrm{div}(f_2) + \mathrm{div}(f_3)$이고 $\mathrm{div}(f_3) = \mathrm{div}(l) - \mathrm{div}(v)$이기 때문에 사실이다. 여기서

$$\begin{aligned} \mathrm{div}(l) &= (P_1) + (P_2) + (-P_3) - 3(\mathcal{O}) \\ \mathrm{div}(v) &= (P_3) + (-P_3) - 2(\mathcal{O}) \end{aligned}$$

이다.

만일 $P_1, P_2 \in E(K)$이고 $f_1, f_2 \in K(E)$이면 $P_3 \in E(K)$이고 $f_3 \in K(E)$이다. 모든 계산은 체 K 자체에서 일어난다. f_3 ($K(x,y)$의 원소로서) 는 P_3와 $-P_3$점에만 정의되지 않고, $1/f_3$ (역시 $K(x,y)$의 원소로서)는 $P_1, P_2, -P_3$에서 정의되지 아니한다. (만일 우리가 f_3를 유리 함수로서 취급한다면, $\mathrm{div}(f_3) = (P_1) + (P_2) - (\mathcal{O})$이므로 f_3가 정의되지 아니하는 E 상의 유일한 점은 P_3와 $(\mathcal{O})$이다.)

그러면 $D = \sum_{i=1}^{n} a_i(P_i)$를 주 인수라고 하자. $D = \mathrm{div}(f)$가 되도록 $f \in \overline{K}(E)$를 찾을 수 있다.

(i) $D = \sum_{i=1}^{n} a_i((P_i) - (\mathcal{O}))$로 쓴다. 이것은 D의 차수가 0 이므로 가능하다.

(ii) 각 $i, 1 \leq i \leq n$에 대하여 다음과 같은 $P_i' \in E$와 $f_i \in \overline{K}(E)$를 계산한다.

$$a_i((P_i) - (\mathcal{O})) = (P_i') - (\mathcal{O}) + \mathrm{div}(f_i)$$

$1 = d_1, d_2, \ldots, d_t = a_i$는 a_i의 고정된 addition chain이라고 하자. 즉, 각 $d_j, j \geq 2$는 $k < j, l < j$ 에 대하여 $d_j = d_k + d_l$로 얻어진다. $t \leq 2r, r = \lceil \log_2 a_i \rceil$ 길이의 a_i에 대한 addition chain은 반드시 존재한다. canoical

form으로 인수를 더하는 방법을 이용하여, $d_j((P)-(\mathcal{O}), j=1,2,\ldots,T$에 대한 canonical form을 계산할 수 있다.

$$f_i = \prod_k \left(\frac{l_k}{v_k}\right)^{b_k} \tag{5.2}$$

여기서 l_k, v_k는 $\overline{K}(E)$에서 선형 다항식이다. 또한, 식 (5.2)에서 곱 연산에서 l_k/v_k 항의 수는 최대 $2r$이고 각 exponent b_k는 최대 2^{2r} 이다.

(iii) 그러면, 인수 $(P_i')-(\mathcal{O})+\mathrm{div}(f_i), 1\le i\le n$을 더한다.

만일 $P_i\in E(K)$이면 $f\in K(E)$이고 모든 연산은 K 상에서 이루어 진다.

K가 유한체라고 가정하고 각 $P_i\in E(K)$이라 하자. 이 알고리즘의 문제는 이항 유리 함수 f이 입력의 크기에 비하여 exponential 크기 일 수도 있다는 것이다. f를 explicit하게 쓰는 것보다는 f를 인수분해한 형태(factored form)로 둔다. (ii) 에 의해, 각 f_i는 factored form으로 f는 다항식 크기를 가진다는 것을 알 수 있다. 더욱이, 이 방법은 다항식 시간을 갖는다. f는 점 P에서 ($f(P)$ 가 주어진다면) 계산될 수 있다.

중간 인수의 canonical form이 $D_j=(Q_j)-(\mathcal{O})+\mathrm{div}(g_j)$로 하자. 그러면 f ($K(x,y)$의 원소로서) 는 $\pm Q_j$점에서 정의될 수 없다. Weil pairing를 계산하는 알고리즘을 이용하면 계산할 수 있다.

예 5.1 *F_{13}에서 정의된 $y^2=x^3+7x$를 생각하자. 표 (5.1)에는 $E(F_{13})$의 점과 위수를 각각 표시하였다. 이 표로부터 $\#E(F_{13})=18$이고 $E(F_{13})\cong Z_6\oplus Z_3$이다*

$D=6(P_8)-6(\mathcal{O})$라 하자. 이것은 주 인수이다. $\mathrm{div}(f)=D$가 되도록 유리 함수 f를 찾아 보자.

$$\begin{aligned}
(P_8)-(\mathcal{O}) &= (P_8)-(\mathcal{O})+\mathrm{div}(1).\\
2(P_8)-2(\mathcal{O}) &= [(P_8)-(\mathcal{O})]+[(P_8)-(\mathcal{O})]\\
&= (P_7)-(\mathcal{O})+\mathrm{div}(\frac{-x+y+3}{x-4})\\
4(P_8)-4(\mathcal{O}) &= [2(P_8)-2(\mathcal{O})]+[2(P_8)-2(\mathcal{O})]\\
&= (P_6)-(\mathcal{O})+\mathrm{div}\left(\frac{(-x+y+3)^2}{(x-4)^3}\frac{(5x+y+7)}{(x-4)}\right)
\end{aligned}$$

표 5.1: $E : y^2 = x^3 + 7x$에서 F_{13} 유리점

점	위수	점	위수
$P_0 = \mathcal{O}$	1	$P_9 = (5, 11)$	6
$P_1 = (0, 0)$	2	$P_{10} = (8, 3)$	6
$P_2 = (2, 3)$	6	$P_{11} = (8, 10)$	6
$P_3 = (2, 10)$	6	$P_{12} = (9, 5)$	3
$P_4 = (3, 3)$	3	$P_{13} = (9, 8)$	3
$P_5 = (3, 10)$	3	$P_{14} = (10, 2)$	3
$P_6 = (4, 1)$	3	$P_{15} = (10, 11)$	3
$P_7 = (4, 12)$	3	$P_{16} = (11, 2)$	6
$P_8 = (5, 2)$	3	$P_{17} = (11, 11)$	6

$$\begin{aligned} 6(P_8) - 6(\mathcal{O}) &= [2(P_8) - 2(\mathcal{O})] + [4(P_8) - 4(\mathcal{O})] \\ &= \operatorname{div}\left(\frac{(-x+y+3)^3}{(x-4)^3} \frac{(5x+y+7)}{(x-4)} \frac{(x-4)}{1} \right). \end{aligned}$$

따라서 원하는 함수는 factored form으로

$$f = \frac{(-x+y+3)^3}{(x-4)^3}(5x+y+7)$$

이다. $F_{13}(x, y)$의 원소로서 f는 P_6와 P_7에서 정의되지 아니한다. 그러나, 유리함수로서 생각한다면, 이 점에서 정의될 수 있다. 이것은 다음과 같이 이유이다.

$$\begin{aligned} f &= \frac{(-x+y+3)^3}{(x-4)^3} \frac{(x+y-3)^3}{(x+y-3)^3}(5x+y+7) \\ &= \frac{(y^2 - x^2 + 6x - 9)^3}{(x-4)^3} \frac{(5x+y+7)}{(x+y-3)^3} \\ &= \frac{(x^3 + 7x - x^2 + 6x - 9)^3}{(x-4)^3} \frac{(5x+y+7)}{(x+y-3)^3} \\ &= \frac{(x^3 - x^2 + 4)^3}{(x-4)^3} \frac{(5x+y+7)}{(x+y-3)^3} \\ &= \frac{(x-4)^3(x-5)^6}{(x-4)^3} \frac{(5x+y+7)}{(x+y-3)^3} \end{aligned}$$

$$= (x-5)^6 \frac{(5x+y+7)}{(x+y-3)^3}$$

이로서 확실히 P_6와 P_7에서 정의될 수 있다.

1.3 Weil pairing의 계산

m은 p와 서로 소인 정수이고 $P, Q \in E[m]$이라 하자. $e_m(P,Q)$를 계산하자. 2점 $T, U \in E$를 $P+T \neq U, Q+U$ 그리고 $T \neq U, Q+U$되도록 선택한다. $A = (P+T)-(T)$라 하고

$$A-(P)+(\mathcal{O}) = (P+T)-(T)-(P)+(\mathcal{O}) \in D_l$$

이므로 $A \sim (P)-(\mathcal{O})$ 이다. 유사하게, $B = (Q+U)-(U)$라 하면, $B \sim (Q)-(\mathcal{O})$ 이다.

$f_A, f_B \in \overline{K}(E)$가

$$\mathrm{div}(f_A) = m(P+T) - m(T) \mathrm{div}(f_B) = m(Q+U) - m(U)$$

이라고 한다. f_A, f_B는 전술한 방법으로 계산 할 수 있다. 그러면

$$e_m(P,Q) = \frac{f_A(B)}{f_B(A)} = \frac{f_A((Q+U)-(U))}{f_B((P+T)-(T))} = \frac{f_A(Q+U)f_B(T)}{f_A(U)f_B(P+T)}$$

이다. $e_m(P,Q)$는 T와 U의 선택에 의하여 정의된다는 것을 주의하자. 만일 $P, Q \in E(K)$이면 $T, U \in E(K)$를 선정하고 $f_A, f_B \in K(E)$이고 모든 연산은 K 체 상에서 이루어 진다.

K가 유한 체이라고 가정하고 $P, Q \in K(E)$이고 $T, U \in E(K)$로 선택한다. 유리 함수 f_A, f_B는 입력의 크기에 비하여 지수함수적으로 크게된다. 따라서, f_A와 f_B는 factored form으로 표현한다.

m에 대한 addition chain $1 = a_1, a_2, \ldots, a_t = m$이라고 하자. $R \in E(K)$이고 f는 전술한 방법으로 계산한 함수하고 하자. 여기서

$$m(R) - m(\mathcal{O}) = (P') - (\mathcal{O}) + \mathrm{div}(f)$$

이다. 중간 인수는 $(a_i R) - (\mathcal{O}) + \mathrm{div}(f_i), 1 \leq i \leq t$ 이다. $K(x,y)$의 원소로 f는 최대 모든 점 $\pm a_1 R, \pm a_2 R, \ldots, \pm a_t R$에 대하여 정의되지 아니 할 수도 있다.

유리함수로서 f_A는 U와 $Q+U$에서 정의된다. 그러나, $K(x,y)$의 원소로서 f_A는 U와 $Q+U$에서 정의가 않되는 경우도 있다. f_A가 ($K(x,y)$의 원소

로서) 점 $Q+U$와 U에서 정의되는 것을 보증하기 위하여는 U와 $Q+U$가 $\pm a_1T, \pm a_2T, \ldots, \pm a_tT, \pm a_1(P+T), \pm a_2(P+T), \ldots, \pm a_t(P+T)$와 다르게 되도록 U를 선정한다. 고정된 T에 대하여는 이 조건을 만족하지 아니하는 점 U의 수는 최대 $8t$이다. 유사하게, f_B가 $P+T$와 T에서 정의되는 것을 보장하기 위하여는 T와 $P+T$가 $\pm a_1U, \pm a_2U, \ldots, \pm a_tU, \pm a_1(Q+U), \pm a_2(Q+U), \ldots, \pm a_t(Q+U)$와 다르게 되도록 T를 선정한다. 고정된 U에 대하여 이 조건을 만족하지 아니하는 점 T의 수는 최대 $8t$이다. 따라서, $(T,U) \in E(K) \times E(K)$가 이 조건을 만족하지 아니하는 점의 수는 최대 $16t\#E(K)$이다. 길이 $t \leq 2\log_2 m$을 가진 m의 addition chain은 반드시 존재하므로 좋은 쌍 (T,U)를 선정할 확률은 $m \geq 1024$일 때 $1/2$ 보다 크다.

결국, 확률적 다항식 시간에 타원 곡선상에 랜덤 점을 선택할 수 있으므로 K가 유한체이면 $e_m(P,Q)$를 계산하는 알고리즘은 확률적 다항식 시간을 가진다.

예 5.2 *$E/F_{13} : y^2 = x^3+7x$를 고려하자. $P = P_4 = (3,3)$이고 $Q = P_6 = (4,1)$이라 하자. $e_3(P,Q)$를 계산하자.*

랜덤 점 $T = (8,3)$, $U = (5,20)$를 우선 선택하고 $P+T = (2,10)$, $Q+U = (5,11)$를 계산한다. 다음과 같이 canonical form으로 인수를 표현하자.

$$\begin{aligned}
3(P+T) - 3(\mathcal{O}) &= (P_1) - (\mathcal{O}) + div(\frac{(8x+y)(x+y+1)}{x(x+3)}).\\
3(T) - 3(\mathcal{O}) &= (P_1) - (\mathcal{O}) + div(\frac{(11x+y)(8x+y+11)}{x(x+4)}).\\
3(Q+U) - 3(\mathcal{O}) &= (P_1) - (\mathcal{O}) + div(\frac{(3x+y)(x+y+10)}{x(x+9)}).\\
3(U) - 3(\mathcal{O}) &= (P_1) - (\mathcal{O}) + div(\frac{(10x+y)(12x+y+3)}{x(x+9)}).
\end{aligned}$$

f_A와 f_B가 $div(f_A) = 3(P+T) - 3(T)$, $div(f_B) = 3(Q+U) - 3(U)$인 함수라는 것을 상기하자. 첫 번째 2개의 방정식을 빼면

$$f_A = \frac{(8x+y)(x+y+1)(x+4)}{(x+3)(11x+y)(8x+y+11)}$$

마지막 2개의 방정식을 빼면

$$f_B = \frac{(3x+y)(x+y+10)}{(10x+y)(12x+y+3)}$$

결국

$$e_m(P,Q) = \frac{f_A(Q+U)}{f_A(U)}\frac{f_B(T)}{f_B(P+T)} = 9$$

이다. 원소 9는 F_{13}에서 위수로 3을 가짐을 주의하라.

제 2 절 타원 곡선 대수 문제를 유한체 대수 문제로 축소

다음의 결과는 [63]에서 나온 것으로 타원곡선 $E(F_q)$의 점을 최대 위수의 점 P에 의해 생성된 부분 군 $E(F_q)$의 $< \mathrm{P} >$의 coset으로 나누는 방법을 제시한다.

보조정리 5.1 *$E(F_q)$은 group type (n_1, n_2)을 가진 타원 곡선이라고 하고, P를 최대 위수 n_1을 가진 원소라고 하자. 그러면, 모든 점 $P_1, P_2 \in E(F_q)$에 대하여 만일 $e_{n_1}(P, P_1) = e_{n_1}(P, P_2)$이어야만 P_1과 P_2는 $< P >$의 동일한 coset에 존재한다.*

다음의 결과는 위와 유사하나 완전함을 위하여 기술한다.

보조정리 5.2 *$E(F_q)$가 $E[n] \subseteq E(F_q)$인 타원 곡선이라고 하자. 단, n와 p가 서로 소인 양의 정수이다. $P \in E[n]$이 위수 n인 점이라고 하자. 모든 $P_1, P_2 \in E[n]$에 대하여 만일 $e_n(P, P_1) = e_n(P, P_2)$이라면 $E[n]$안에 $< P >$의 동일한 coset에 존재한다.*

Proof: 만일 $P_1 = P_2 + kP$이면,

$$\begin{aligned} e_n(P, P_1) &= e_n(P, P_2)e_n(P, P)^k \\ &= e_n(P, P_2) \end{aligned}$$

역으로 P_1과 P_2이 $E[n]$상에 $< \mathrm{P} >$의 다른 coset에 있다고 하자. 그러면, $P_1 - P_2 = a_1P + a_2Q$로 할 수 있다. 여기서 (P, Q)는 $a_2Q \neq \mathcal{O}$이고 $E[n] \cong Z_n \oplus Z_n$에 생성되는 쌍이다. 만일 $b_1P + b_2Q$가 $E[n]$의 임의의 점이라면,

$$\begin{aligned} e_n(a_2Q, b_1P + b_2Q) &= e_n(a_2Q, P)^{b_1}e_n(Q, Q)^{a_2b_2} \\ &= e_n(P, a_2Q)^{-b_1} \end{aligned}$$

만일 $e_n(P, a_2Q) = 1$이면 e_n의 non-degeneracy 성질에 의하여 $a_2Q = \mathcal{O}$이다. 이것은 모순이다. 따라서 $e_n(P, a_2Q) \neq 1$이다. 결국

$$\begin{aligned} e_n(P, P_1) &= e_n(P, P_2)e_n(P, P)^{a_1}e_n(P, a_2Q) \\ &\neq e_n(P, P_2) \end{aligned}$$

□

참조를 위하여 다음의 결과를 언급한다.

보조정리 5.3 *G는 군이고, $\alpha \in G$라 하자. $n = \prod_{i=1}^{k} p_i^{\beta_i}$는 n의 소인수 분해라고 하자. 그러면, α는 위수 n을 가지는 필요 충분 조건은*

$$\begin{aligned} &(i) \quad \alpha^n = 1 \qquad and \\ &(ii) \quad \alpha^{n/p_i} \neq 1 \qquad for\ each\ i, 1 \leq i \leq k. \end{aligned}$$

보조정리 5.4 *G는 type (cn, cn)의 아벨 군이라고 하자. 만일 요소 $\{a_i\}$를 G로부터 균일하고 램덤하게 선택한다면, $\{ca_i\}$는 type (n, n)를 가진 G의 부분 군의 요소에서 균일하게 분포한다.*

2.1 축소

$E(F_q)$를 군 구조 $Z_{n_1} \oplus Z_{n_2}$ $(n_1|n_2)$ 를 가진 유한체 F_q상의 타원곡선이라고 하자. $E(F_q)$의 정의된 방정식으로 부터 Schoof 알고리즘[136]에 의하여 $\#E(F_q)$는 다항식 시간에 계산할 수 있다. 또한 $\gcd(\#E(F_q), q-1)$의 소인수 분해가 주어진다면, 후술할 4절에서 제시하는 알고리즘에 의하여 확률적 다항식 시간으로 n_1과 n_2를 결정할 수 있다. 만일 $\gcd(\#E(F_q), q) = 1$ 가정하면 $E[n_1] \cong Z_{n_1} \oplus Z_{n_1}$이다.

$P \in E(F_q)$가 위수 n의 점이고 n은 n_1의 divisor이고 $R \in E(F_q)$리 하자. n이 알려져 있다고 하면 타원 곡선 대수 문제는 다음과 같다 : 주어진 P와 R로 부터 $R = lP$가 되도록 유일한 정수 $l, 1 \leq l \leq n-1$을 (만일 그러한 정수가 존재한다면) 결정하라.

$e_n(P, P) = 1$이므로 Lemma 5.1으로 부터 $nR = \mathcal{O}$ 그리고 $e_n(P, R) = 1$이면 $R \in < P >$임을 유도할 수 있다.

P가 최대 위수를 가진 경우, 체 F_q 자체에서 이산 대수 문제를 풀어서 l에 대한 부분 정보를 찾는 알고리즘을 기술하자.

Algorithm 1

Input : An element $P \in E(F_q)$ of maximun order n_1, and $R = lP$.

Output : An integer $l' \equiv l \pmod{n'}$ where n' is a divisor of n_2.

Step 1. Pick a random point $T \in E(F_q)$.

Step 2. Compute $\alpha = e_{n_1}(P, T)$ and $\beta = e_{n_1}(R, T)$.

Step 3. Compute l', the discrete logarithm of β to the base of α in F_q.

정리 5.1 *Algorithm 1은 n'이 n_2의 어떤 divisor이면 $l' \equiv l \pmod{n'}$을 옳바르게 계산한다.*

Proof: $G \in E(F_q)$이고 2개의 점 (P, Q)가 $E(F_q)$를 생성하는 위수 n_2의 원소라고 하자. 그러면, $T = c_1P + c_2G$이라고 하자. 그러면,

$$\alpha^{n_2} = e_{n_1}(P, T)^{n_2} = e_1(P, P)^{c_1 n_2} e_{n_1}(P, c_2 n_2 G) = e_{n_1}(P, \mathcal{O}) = 1$$

α의 위수가 n'으로하고 n_2를 나눈다고 하자. $n_1 | q - 1$ 이므로 $\alpha \in F_q$이다. 그리하여

$$\beta = e_{n_1}(R, T) = e_{n_1}(lP, T) = e_{n_1}(P, T)^l = \alpha^l = \alpha^{l'}$$

이므로 F_q 상에서 기저 α의 β의 이산 대수를 계산함으로서 l'을 계산할 수 있다. □

$\#E(F_q)$ 내에 $<$ P $>$의 n_2 coset이 있으므로, Lemma (5.1)으로 부터 $n' = n$의 확률은 $\phi(n_2)/n_2$임을 유도할 수 있다. 만일 n_2가 n_1에 비하여 적다면 (만일 곡선이 랜덤하게 선택된다면 $n_2 | \gcd(n_1, q-1)$의 가능성이 기대된다.) 이 방법은 l에 대하여 의미 있는 정보를 제공하지 못한다. 추후에 $l \pmod{n}$을 계산하는 방법을 기술한다.

정리 5.2 *$P \in E$가 위수 n의 점이라고 한다. $Q \in E[n]$이 존재하여 $e_n(P, Q)$가 primitive n-th root of unity이다.*

Proof: $Q \in E[n]$이라하고 Weil pairing의 bilinearity에 의하여 다음을 얻는다.

$$e_n(P, Q)^n = e_n(P, nQ) = e_n(P, \mathcal{O}) = 1$$

따라서, $e_n(P, Q) \in \mu_n$ 단, μ_n은 F_{q^k}상에서 n-th roots of unity의 부분 군을 나타낸다.

$E[n]$에는 $<$ P $>$의 n coset이 있다. Lemma (5.2)에 의하여 Q가 이런 n coset의 대표원에 따라 변화할 때, $e_n(P,Q)$는 mu_n의 모든 원소에 따라 변화한다. 따라서 결과는 만족한다. □

$Q \in E[n]$이라하고 $e_n(P,Q)$는 primitive n-th root of unity라고 한다. 다음 정리의 증명은 당연하다.

정리 5.3 *$f :< P >\rightarrow \mu_n$은 $f : R \mapsto e_n(R,Q)$로 정의된다. 그러면, f는 군 동형이다.*

따라서 타원 곡선의 이산 대수 문제를 유한체 상의 이산 대수 문제로 축소하는 방법을 서술 할 수 있다.

Algorithm 2

Input: An element $P \in E(F_q)$ of order n, and $R \in< P >$.

Output : An integer l such that $R = lP$.

Step 1. Determine the smallest integer k such that $E[n] \subseteq E(F_{q^k})$

Step 2. Find $Q \in E[n]$ such that $\alpha = e_n(P,Q)$ has order n.

Step 3. Computer $\beta = e_n(R,Q)$.

Step 4. Compute l, the discrete logarithm of β to the base α in F_q.

Algorithm 2이 옳는 것은 다음과 같다.

$$\beta = e_n(R,Q) = e_n(lP,Q) = e_n(P,Q)^l = \alpha^l$$

Remark

Algorithm 2는 k가 일반적으로 지수적으로 크게 되면 일반적으로 ($\ln q$의) 지수함수 시간을 갖는다. Algorithm 2는 K를 결전하는 방법과 Q를 찾는 방법이 제공되지 아니하였으므로 완전한 것은 아니다. 다음에 초특이 타원 곡선류에서 이것을 언급하자.

예 5.3 $E/F_{13} : y^2 = x^3+7x$*를 생각하자.* $P = (3,3), Q = 2P = (3,10)$*이라 하자. Algorithm 2의 표기에 의하여* $n = 3$*을 얻는다.* $E[3] \subseteq E(F_{13})$ *이므로* $k = 1$*이다.* $Q = (4,1)$*을 선택한다. 예 (5.2)에 의하여*

$$\alpha = e_3(P,Q) = 9$$

를 얻고 위수는 3이다. 유사한 계산으로

$$\beta = e_3(R,Q) = 3$$

을 얻는다. $9^2 \equiv 3 \pmod{13}$*이므로* $\log_P R = 2$*를 얻는다.*

2.2 초 특이 곡선

Algorithm 2를 초특이 타원 곡선의 경우, 확률적 다항식 시간으로 축소 문제를 토의한다. 유한체에서 이산 대수 문제를 위한 준 지수 시간의 알고리즘과 혼합하면, 초 특이 곡선에 있어서 타원 곡선 알고리즘을 계산하는 확률적 준 지수 시간의 알고리즘을 얻을 수 있다.

$E(F_q)$는 F_q 상의 위수 $q+1-t$의 초특이 타원 곡선이라고 하고 $q = p^m$ 이라 한다. 그러면 E는 다음의 분류 중 하나의 곡선이다.

I $t = 0, E(F_q) \cong Z_{q+1}$.

II $t = 0, E(F_q) \cong Z_{(q+1)/2} \oplus Z_2$, $q \equiv 3 \pmod{4}$.

III $t^2 = q$ (and m is even.)

IV $t^2 = 2q$ (and $p = 2$ and m is odd.)

V $t^2 = 3q$ (and $p = 3$ and m is odd.)

VI $t^2 = 4q$ (m is even.)

P는 $E(F_q)$에서 위수 n의 점이라고 하자. $n_1|(q+1-t)$,$p|t$이므로 $\gcd(n_1, q) = 1$을 얻는다.

Weil 정리와 보조정리 2.13을 이용하면, $E[n_1] \subseteq E(F_{q^k})$ 이 되도록 하는 최소의 양 정수 k를 결정할 수 있다. 다음은 (IV)류의 곡선에 대한 예제 계산을 보여준다.

보조정리 5.5 *(IV)류의 타원 곡선은 $k = 4$를 얻는다.*

Proof: $q = 2^m$ (m odd) 이고 $\#E(F_q) = n = q + 1 + \sqrt{2q}$ 라고 한다. ($n = q + 1 - \sqrt{2q}$인 경우도 유사하게 취급 가능하다.) 보조정리 2.13(iii)에 의하여 $E(F_q)$는 순환군이다. 그러면 Weil theorem을 이용하면 $\#E(F_{q^2}) = q^2 + 1$과 $\#E(F_{q^3}) = q^3 + 1 - \sqrt{2q^3}$을 얻는다. 보조정리 2.13(iii)에 의하여 $E(F_q^2)$는 순환군이고, 보조정리 2.13(i)에 의하여 $E(F_q^3)$는 순환군이다. 결국

$$E(F_{q^2}) \bigcap E[n] = E(F_q)$$

와

$$E(F_{q^3}) \bigcap E[n] = E(F_q)$$

가 된다. 결국, $\#E(F_q^4) = q^4 + 1 + 2\sqrt{q^4}$가 된다. 보조정리 2.13(ii)에 의하여 $\#E(F_{q^4}) \cong Z_{q^2+1} \oplus Z_{q^2+1}$을 얻는다. $q^2 + 1 = (q + 1 + \sqrt{2q})(q + 1 - \sqrt{2q})$ 이므로 $E[n] \subseteq E(F_{q^4})$가 된다. □

편의 상, 초특이 곡선에 대하여는 다음의 2개 표로 정리한다.

표 5.2: 초특이 타원 곡선에 대한 정보

곡선 류	t	군 구조	n_1	k
I	0	cyclic	$q+1$	2
II	0	$Z_{(q+1)/2} \oplus Z_2$	$(q+1)/2$	2
III	$\pm\sqrt{q}$	cyclic	$q+1 \mp \sqrt{q}$	3
IV	$\pm\sqrt{2q}$	cyclic	$q+1 \mp \sqrt{2q}$	4
V	$\pm\sqrt{3q}$	cyclic	$q+1 \mp \sqrt{3q}$	6
VI	$\pm 2\sqrt{q}$	$Z_{\sqrt{q}\mp 1} \oplus Z_{\sqrt{q}\mp 1}$	$\sqrt{q} \mp 1$	1

각 곡선 류에서 $E(F_{q^k})$의 구조는 적절한 c에 대하여 $Z_{cn_1} \oplus Z_{cn_1}$의 형태를 가지고 있다. 그러면, 초특이 곡선에 대하여 축소에 관한 상세한 결과를 다음에 기술한다.

Algorithm 3

Input: An element P of order on a supersingular curve $E(F_q)$ and $R \in < P >$.

표 5.3: 초특이 타원 곡선에 대한 정보

곡선 류	$E(F_{q^k})$의 type	c
I	$(q+1, q+1)$	1
II	$(q+1, q+1)$	2
III	$(\sqrt{q^3} \mp 1, \sqrt{q^3} \pm 1)$	$\sqrt{q} \pm 1$
IV	(q^2+1, q^2+1)	$q \pm \sqrt{2q} + 1$
V	(q^3+1, q^3+1)	$(q+1)(q \pm \sqrt{3q} + 1$
VI	$(\sqrt{q} \mp 1, \sqrt{q} \mp 1)$	1

Output : An integer l such that $R = lP$.

Step 1. Determine k and c from Tables (5.2) and (5.3).

Step 2. Pick a random point $Q' \in E(F_{q^k})$ and set $Q = (cn_1/n)Q'$

Step 3. Compute $\alpha = e_n(P, Q)$ and $\beta = e_n(R, Q)$.

Step 4. Compute the discrete logarithm l' of β to the base α in F_{q^k}.

Step 5. Check whether $l'P = R$. If this is so, then $l = l'$ and we are done. Otherwise, the order of α must be less than n, so go to **Step 2**.

보조정리 (5.2)에 의하면 Q는 $E[n]$상의 랜덤 점이라는 것을 주목한다. 또한, 체 원소 α가 위수 n을 가질 확률은 $\phi(n)/n$이다. 보조정리 (5.2)와 F_{q^k}에는 위수 n의 $\phi(n)$의 원소가 있다는 사실로 부터 $E[n]$내에는 $< P >$의 n coset이 있다.

다음은 Algorithm 3이 ($\ln n$에 대한) 확률적 다항식의 축소라는 것을 제시한다.

정리 5.4 *만일 $E(F_q)$가 초특이 곡선이라면, $E(F_q)$ 상의 이산 대수 문제를 F_q로의 축소는 ($\ln n$에 대한) 확률적 지수 시간의 축소이다.*

Proof: 소수 체 상의 F_q의 기저가 확실히 주어져 있다고 가정한다. F_{q^k} 상의 연산을 위하여는 F_q 상의 차수 k의 기약 다항식 $f(x)$ 가 필요하다. 이것은 [10]에서 주어진 방법으로 확률적 다항식 시간에 행해 진다. 그러면 $F_{q^k} \cong F_q[x]/(f(x))$가

되고 $(f(x))$는 $f(x)$에 의하여 생성된 ideal 을 지칭한다. $F_q[x]$에서 상수 다항식은 F_q에 동형인 부분군이 된다.

$Q' \in E(F_{q^k})$, $k \leq 6$이므로 점 Q'는 확률적 다항식 시간에 결정된다. Miller의 알고리즘에 의하여, 원소 α, β는 확률적 다항식 시간에 계산된다.

$$\frac{n}{\phi(n)} \leq 6 \ln \ln n, \text{ for } n \geq 5$$

이므로[131], $e_n(P,Q)$가 위수 n을 가지도록 하는 Q를 찾기 까지의 반복의 기대값은 $O(\ln \ln n)$이다. 결국, $l'P = R$은 다항식 시간에 검증되고, $n = O(q)$가 된다. □

Algorithm 3의 Step 4에서 푸는 F_{q^k}상의 이산 대수 문제는 위수 n,$(n < q^k - 1)$의 기저 원소 α를 가질 수가 있다. 유한체에서 이산 대수문제를 푸는 Index calculus 방법은 확률적 준 지수 시간 알고리즘으로 기저 원소가 primitive이어야 한다. 이것을 이용하면 다음을 얻는다.

따름정리 5.1 *P는 초특이 타원 곡선 $E(F_q)$에서 위수 n의 원소라고 하고, $R = lP$는 $E(F_Q)$ 상의 점이라고 한다. 만일 q가 소수, 또는 q가 소수의 멱승 고정된 p에 대하여 $q = p^m$이면 Algorithm 3은 확률적 준 대수 시간에 l을 결정할 수 있다.*

Proof: F_{q^k} 상에서 기저 α에 대한 β의 대수를 찾는 문제는 다음과 같이 준 지수 시간에 계산된다.

우선, 소인수 분해 방법 (예를들면, 경험적 수행 시간 분석에 의한 실제적인 알고리즘 [79] 또는 [142], 엄밀한 수행 시간 분석에 의한 알고리즘 [82], [125]에 의함) 의 여러가지 방법 중 에 하나를 이용하여, $q^k - 1$의 소인수를 구한다. 다음에 $q^k - 1$의 부분 인수 분해를 구한다 :

(I) $q^2 - 1 = (q+1)(q-1)$

(II) $q^2 - 1 = (q+1)(q-1)$

(III) $q^3 - 1 = (q-1)(q+1-\sqrt{q})(p+1+\sqrt{q})$

(IV) $q^4 - 1 = (q-1)(q+1)(q+1-\sqrt{2q})(q+1+\sqrt{2q})$

(V) $q^6 - 1 = (q-1)(q+1)(q+1-\sqrt{3q})(q+1+\sqrt{3q})(q^2+q+1)$

그리고 F_{q^k} 상에 랜덤 요소 λ가 위수 q^k-1이 되도록 랜덤하게 선택한다. 기대되는 시행 횟수는 $(q^k-1)/(\phi(q^k-1)$ 이며, 이것은 $k \leq 6$이므로 $O(\ln \ln q)$이다. λ의 위수는 보조정리 (5.3)에 의하여 다항식 시간에 검증된다. F_{q^k} 상에서 2개의 이산 대수 문제를 풀어서, 유일한 정수 s와 t $(0 \leq s,t \leq^k -1)$를 $\alpha = \lambda^s$, $\beta = \lambda^t$가 되도록 구할 수 있다.

$\beta = \alpha^{l'}$이므로 $sl' \equiv t \pmod{q^k-1}$의 합동식을 구한다. $w = \gcd(s, q^k - 1)$라 하고, $v = (q^k-1)/w$를 α의 위수라고 놓는다. 그러면, $l' = (s/w)^{-1}(t/w) \pmod{v}$가 된다.

F_{q^k}의 대수 문제는 예를들면 [30]에 있는 알고리즘을 이용하면 소수 q와 $k = 1$,소수 q와 $k > 1$, 한 소수의 멱승 q, 경우에 $\ln q^k$의 준 지수 시간 함수 계산된다. □

실제 타원 곡선의 대수 문제를 해결하려면, n을 소인수 분해하여야 한다. 소인수를 이용하여 α의 위수를 쉽게 검증한다. Q를 찾기 위하여는 α가 위수 n을 가질 때 까지 $E[n]$상에 랜덤 점을 반복적으로 선택한다.

l'이 실제로 l이 되기 전까지 몇개의 이산 대수 문제를 풀어야 하는 가능성을 피할 수 있다. 이 방법은 Algorithm 3에서 제시한 방법과는 다르고, 유한체에서 이산 대수 문제로 확률적 다항식 시간의 축소가 아니다.

전 절에서 서술한 알고리즘의 주된 부분은 F_{q^k}에서 이산 대수를 계산하는 마지막 단계이다. 정수 n에 대한 소인수 분해 방법 중 수체 선별법 [79]는 수행 시간의 기대치는 $L[n, c, 1/3]$이다. 따라서 수행 시간의 기대치는 F_{q^k}에서 이산 대수 문제를 푸는 가장 좋은 알고리즘의 수행 시간에 의존하여 $L[q^k, c, 1/2]$ 또는 $L[q^k, c, 1/3]$이 된다.

결론으로 초특이 타원 곡선의 경우에는 이전에 믿었던 것 보다 타원 곡선의 이산대수 문제는 훨씬 더 쉽게 풀 수 있게 된다.

2.3 비 초타원 곡선

E를 지표 p의 체 F_q 상의 정의된 비 초특이 곡선이라고 하자. $P \in E(F_q)$는 위수 n의 점이고, $R \in < P >$라고 하자. $\log_P R$을 계산하는 Algorithm 2는 $\gcd(n, q) = 1$ 인 경우에만 유효하다. 그러나 $\gcd(n, q) \neq 1$인 경우에도 다음과 같이 쉽게 확장된다.

$n = p^s n', s \geq 1$이고 $\gcd(n', p) = 1$이라고 하자. $P' = p^s P$, $R' = p^s R$이라고 하자. 그러면 $R' \in < P' >$이므로 Algorithm 2는 $\log'_P R'$을 계산하는 데 응용될

수 있다.

$$\log'_P R' \equiv \log_P R \pmod{n'} \tag{5.3}$$

그러면, $P'' = n'P, R'' = n'R$라 하자. $\mathrm{ord}(P'') = p^s$이고 $R'' \in < P'' >$를 주의한다. Pohlig-Hellman 방법을 사용하여 $\log''_P R''$를 구한다.

$$\log''_P R'' \equiv \log_P R \pmod{p^s} \tag{5.4}$$

이 된다. 만일 p가 작으면, $\log''_P R''$의 계산은 효율적이다. (최악의 경우는 $q = p$인 때 발생) 결국, 식(5.3)과 식(5.4)에 CRT를 적용하면 $\log_P R$을 구한다.

$\gcd(n, q) = 1$이라고 가정한다. F_q 상에서 이산 대수 문제를 푸는 최량의 알고리즘의 수행 시간을 $L[q, c, 1/3]$이라고 하면, Algorithm 2는 $E(F_q)$ 상의 대수 문제를 F_{q^k}상의 문제로 축약된다. 이 문제는 $L[q^k, c, 1/3]$의 복잡도를 가지고 있다. $\ln q$ 상에서 $L[q^k, c, 1/3]$이 준 지수가 되기 위한 필요조건은 $k \leq (\ln q)^2$이다. $E[n] \subseteq E(F_{q^k})$의 하나의 필요조건은 $n|q^k - 1$이다. 즉, modulo n 아래의 q의 위수는 k의 약수이다. 랜덤한 $n \approx q$에서 $k \leq (\ln)^2$의 가능성은 희박하다. 이 결과는 q와 n이 모두 소수인 경우에[72] 명확하다. 따라서 대부분의 비 초특이 타원 곡선에 대하여 Algorithm 2의 축소 방법은 타원 곡선 대수 문제에 완전히 지수 시간의 알고리즘이 된다.

제 3 절 암호학적 의미

La Macchia와 Odlyzkyo[76]는 index calculus 방법의 Gauss 정수 변형 판을 구현하였다. 결과는 F_p (p는 192 비트)에서 대수 문제는 쉽게 풀 수 있다. 수체 선별법이 Gauss 정수법보다 좋은 점근적 수행 시간을 가지고 있으나, 체 F_p ($p \leq 2^{512}$)에서는 실제적이지 못하다. F_{2^m}에 대하여 Gordon과 McCurley[52]는 m이 약 500인 경우 F_{2^m}의 대수 문제 계산은 상당한 계산 자원이 가용하면 거의 가능하리라고 하였다. 따라서, 유한체에서 이산 대수 문제의 최량의 알고리즘과 최고의 가용한 컴퓨터 자원이 주어 진다면 2^{600}보다 큰 유한체에서는 intractable 하다.

타원 곡선 암호 시스템의 구현에 있어서 제시하였던 초특이 타원 곡선의 4가지 부류에 대하여 언급한다. 모든 이런 곡선은 k가 2이다. 즉, 이 곡선에서의 타원 곡선 대수 문제는 underlying field의 quadratic extension에 의거 대수 문제로 효율적으로 축소된다.

(A) $y^2 + y = x^3 + b$ over F_{2^m}, m odd (Class I)

(B) $y^2 = x^3 - ax$ over F_p, where $p > 3$ is a prime, a is a quadratic non-residue in F_p, and $p \equiv 3 \pmod 4$. (Class I)

(C) $y^2 = x^3 - ax$ over F_p, where $p > 3$ is a prime, a is a quadratic residue in F_p, and $p \equiv 3 \pmod 4$. (Class II)

(D) $y^2 = x^3 + b$ over F_p, where $p > 3$ is a prime, and $p \equiv 2 \pmod 3$ (Class I)

F_{2^m}상의 곡선 $E : y^2 + y = x^3$는 다음 장에서 보듯이 구현에는 특별히 매력적이다. F_{2^m} 상의 E를 사용하는 것은 $F_{2^{2m}}$ 상의 non-zero element의 순환 군을 사용하는 것보다 안전하지 아니한다. 곡선 상의 연산 비용은 $F_{2^{2m}}$ 상의 연산 비용보다 높기 때문에 이런 곡선은 현존하는 시스템에 암호학적 응용에는 단점이 된다. (B), (C), (D)의 곡선에 대하여도 유사한 결론을 얻을 수 있다.

Koblitz[67]가 타원 곡선 암호 시스템의 구현에서 F_{2^m} 상에 곡선 $y^2+y = x^3$을 최초로 제안하였다. [9]에는 저자들은 $m = 61$과 $m = 127$인 경우에 제시하였다. index calculus 방법을 이용하여 체 $F_{2^{122}}$와 $F_{2^{254}}$에 대하여 이산 대수 문제는 해결이 가능하므로 이런 곡선은 암호학적 목적으로는 적합하지 않는다. $m = 91$과 $m = 251$의 특별한 값에 대하여도 [93]에 제안되었다. 이런 곡선도 동일한 이유로 피하여야 한다. Miller[100]에 의하여 곡선류 (B)와 (C)가 제안되었다. [9]에는 곡선류(D)가 구현을 위하여 제안되었으며 Kaliski[62]에 의하여 안전한 의사 난수 발생기를 위하여 제안되었다. 타원 곡선 (B)와 (D)를 167 비트 소수 체상에서 암호 시스템을 제안하였으나[65] 이 시스템도 안전하지 못하다.

$y^2 + y = x^3$의 대체 곡선으로 odd m의 F_{2^m}에 대한 초특이 곡선 $y^2 + y = x^3 + x$와 $y^2 + y = x^3 + x + 1$이다.

만일 비 초특이 곡선이 요구되면, 해당하는 k 값이 충분히 크도록 선택하여야 한다. E를 F_q 상에 정의된 비 초특이 곡선이라고 하자. $P \in E(F_q)$를 위수 n의 점이라고 한다. n은 큰 소수 v에 의하여 나누어 진다고 하자. (이 조건은 Pohlig-Hellman의 이산 대수 공격 방법을 피하기 위하여 필요함) Algorithm 2의 공격을 피하기 위하여는, 충분히 큰 c에 대한 $k > c$를 보증하여야 하고 집합 $E[v]$가 각 l $(1 \le l \le c)$에 대하여 $E(F_{q^l})$에 포함되지 아니하여야 한다는 것을 점검하여야 한다. (충분히 큰 c라는 의미는 F_{q^c} 상의 이산 대수 문제가 intractable하게 취급되는 것을 의미한다.) $E[v] \not\subseteq E(F_q^l)$의 2가지 충분 조건은 v^2가 $\#E(F_{q^l})$를 나누지 못하고, v가 $q^l - 1$을 나누지 못하는 조건이다. 이 조건

은 쉽게 검증된다. 만일 이 조건이 만족되면, 기저 P에 대한 대수 문제를 푸는 최량의 알고리즘은 Pohlig-Hellman 방법이고 수행 시간은 $\sqrt{v}$에 대략적으로 비례한다.

제 4 절 군 구조의 탐색

E는 F_q상의 타원 곡선이라고 하고 $N = \#E(F_q)$라 하자. N의 소인수 분해가 알려져 있다고 가정한다. 또한, $\gcd(N, q) = 1$로 가정한다. $E(F_q)$는 type (n_1, n_2)를 가졌다고 하자. Miller[100]에 의하여 n_1과 n_2를 찾는 알고리즘을 제시한다. 우선 다음을 고찰한다.

보조정리 5.6 *$P, Q \in E(F_q)$이고 $r = lcm(ord(P), ord(Q))$, $\alpha = e_r(P, Q)$이면 $ord(\alpha) | \gcd(r, n_1)$이다.*

Proof: $\mathrm{ord}(P) = a$, $r = ar'$로 하자. 그러면, $Q \in E[ar']$, $P \in E[a]$이다. Weil pairing의 compatible 성질에 의하여

$$\alpha = e_r(P, Q) = e_{ar'}(P, r'Q)$$

일반성을 잃지 않고, $\mathrm{ord}(P) = r$이라고 가정한다.

그러면, (P, R)이 $E[r]$의 생성 쌍이고 c_1, c_2가 $Q = c_1P + c_2P$의 정수라고 하자. $E(F_q)[r] \cong Z_r \oplus Z_l$ (단, $l = \gcd(r, n_2)$)이고 $c_2R = Q - c_1P \in E(F_q)$이므로 $lc_2P = \mathcal{O}$이다. 따라서

$$\begin{aligned} \alpha^l = e_r(P, Q)^l &= e_r(P, c_1P + c_2R)^l \\ &= e_r(P, P)^{c_1 l} e_r(P, lc_2R) \\ &= 1 \cdot e_r(P, \mathcal{O}) = 1 \end{aligned}$$

□

따름정리 5.2 *$P, Q \in E(F_q)$이고 $r = lcm(ord(P), ord(Q))$, $s = ord(e_r(P, Q))$라 하자. 만일 $rs = n$이면 $n_1 = r$ 그리고 $n_2 = s$이다.*

Proof: $r | n_1$d이고 $s | n_2$이므로 자명하다. □

위의 따름정리에 의하여 $E(F_q)$의 군 구조를 계산하는 알고리즘이 다음과 같다.

Input : An equation defining an elliptic curve E over a finite field F_q such that $\gcd(N, q) = 1$ where $N = \#E(F_q)$, and the prime factorization of N is known.

Output : The group type (n_1, n_2) of $E(F_q)$.

Step 1. Pick $P, Q \in E(F_q)$ at random

Step 2. Compute $\mathrm{ord}(P), \mathrm{ord}(Q)$ (using the factorization of N) and $r = \mathrm{lcm}(\mathrm{ord}(P), \mathrm{ord}(Q))$

Step 3. Compute $\alpha = e_r(P, Q)$.

Step 4. Compute $s = \mathrm{ord}(\alpha)$

Step 5. If $rs = N$, then output $n_1 = r, n_2 = s$. Otherwise go to **Step 1**.

Step 5의 성공 확률을 분석한다. 우선

$$\Pr(P \text{ has order } n_1) \geq \frac{\phi(n_1)}{n_1}$$

둘째로 보조정리 (5.2)에 의하여

$$\Pr(\alpha \text{ has order } n_2 | P \text{ has order } n_1) = \frac{\phi(n_2)}{n_2}$$

알고리즘이 중지하기 전의 반복 횟수의 기대치는

$$\leq \frac{n_1}{\phi(n_1)} \frac{n_2}{\phi(n_2)} = O((\ln \ln N)^2) = O((\ln \ln q)^2)$$

알고리즘의 각 반복은 확률적 다항식 시간에 수행되므로 알고리즘은 기대되는 다항식 시간에 중지한다.

$\gcd(N, q) = 1$이라는 조건은 이론 전개를 간단히 하기 위하여 가정하였음을 밝혀 둔다. $\gcd(N, q-1)$의 소인수 만을 알고 있다면 이 알고리즘은 확률적 다항식 시간으로 쉽게 동작한다.

제 5 절 참조 사항

Weil pairing의 또 다른 정의와 pairing의 성질 증명에 대하여 [26]과 [142]를 참조한다. 5.1절의 Weil pairing의 계산 알고리즘은 Miller의 미발간 논문[101]에

근거로 하였으며, 4절의 타원 곡선의 군 구조 계산도 마찬가지 이다. 이 알고리즘은 실제로 대단히 유효하다. Zuccherato[154]는 SUN-2 SPARC에 구현하여 $m \approx 200$에 곡선 $E(F_{2^m})$를 계산하는 데 수 분이 소요되었다고 보고하였다.

5.2절의 결과는 [92]로 부터 인용하였으며, IEEE로 부터 허가를 득하여 복사하였다.

5.2.3에서의 축소 알고리즘의 확장은 Miyaji[103]에 의하여 고찰하였으며, F_q 상에 정의된 타원 곡선의 모든 n-torsion point를 찾는 즉, $E[n] \subseteq F(F_q)$ 필요 충분 조건은 [137]에 제시 되었다.

Frey와 Rück[43]은 local field 상에 Abelian variety를 위한 Tate pairing의 변형을 이용하여, (char(F_q)이 n과 서로 소인) F_q 상에 projective irreducible non-singular curve의 divisor class group의 n-torsion part 에서의 대수 문제를 k가 $n|q^k - 1$이 되는 최소의 정수 k에 대하여 F_{q^k} 에서의 이산 대수 문제로의 축소를 제시하였다. 타원 곡선에 대하여 이 방법은 2절의 방법에 비하여 장점이 있다. 왜냐하면 조건 $n|q^k - 1$이 조건 $E[n] \subseteq E(F_{q^k})$보다 통상 약하기 때문이다.

Huang과 Ierardi[57]에서는 ordinary multiple points만을 가진 projective plane 상 principle divisor의 rational function을 구성하는 다항식 시간 알고리즘을 제시하였다.

제 6 장

타원 곡선 암호 시스템의 구현

본 장에서는 유한체 위에 타원 곡선 연산을 수행하는 산술 프로세서의 효율적인 구현 가능성에 대하여 탐색한다. 전술한 바와 같이 곡선과 기반 체 (underlying field)는 현명하게 선정되어야 한다. 그러나, 주어진 기반 체에 대하여도 선택하여야 하는 타원 곡선이 너무도 많다. 초 특이 곡선 상의 대수 문제가 유한체 상의 대수 문제와 정말로 어려운 문제라면, 또는 비 초특이 곡선 상에서 대수 문제가 정말로 untractable 하다면, 여기서 언급하는 시스템은 효율적이고 안전하며 실제 사용에 대단히 매력적이다.

본 장은 다음과 같이 구성되어 있다. 1절에는 F_{2^m}상에서의 효율적인 연산을 제시하였다. 2절에서 5절까지는 ElGamal 암호 시스템을 구현하는 데 비 초특이 타원 곡선을 사용하는 여러가지 방법을 제시한다. 6절에는 초특이 곡선에 대하여도 동일한 점을 토의한다. 7절에는 환 Z_n 상에 타원 곡선을 이용하는 RSA 암호 시스템과 유사한 방법을 연구하고 8절에는 타원 곡선 암호 시스템의 몇가지 구현에 대하여 언급한다.

제 1 절 F_{2^m}상에서 체 연산

표수 2인 유한테 상에 타원 곡선에 대하여 대단히 흥미 있기 때문에 그러한 체에서 산술 연산을 효율적으로 수행하는 기법을 기술한다.

체 F_{2^m}는 F_2 상에서 m 차원 벡터 공간으로 볼 수 있다. 즉, F_{2^m} 상에 m 개 원소의 집합, $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ 이 있어, 각 $\alpha \in F_{2^m}$는 다음과 같이 유일하게 쓸 수 있다.

$$\alpha \;=\; \sum_{i=0}^{m-1} a_i\alpha_i,\ \text{where } \alpha_i \in \{0,1\}$$

그러면 α는 0-1 벡터 $(a_0, a_1, \ldots, a_{m-1})$로 표현된다. 하드웨어로는 원소들이 m 길이의 쉬프트 레지스터에 저장된다. 체 원소의 덧셈은 벡터 표현 상의 bitwise XOR 연산으로 수행되며 1 클럭 사이클 밖에 필요하지 않다.

일반적으로 F_2 상의 F_{2^m}에는 많은 여러가지 기저가 있다. F_2 상의 F_{2^m}의 normal basis 는 다음의 형태를 가진다.

$$\{\beta, \beta^2, \ldots, \beta^{2^{m-1}}\}$$

단, $\beta \in F_{2^m}$이다. 이런 기저가 반드시 존재한다는 것은 알려져 있다 [83]. F_{2^m} 상에 원소 α가 주어지면, $\alpha = \sum_{i=0}^{m-1} a_i\beta^{2^i}$로 쓸 수 있다. 단, $a_i = \{0,1\}$이다. 2승은 F_{2^m} 상에서 선형 연산자이므로

$$\alpha^2 = \sum_{i=1}^{m-1} a_i\beta^{2^{i+1}} = \sum_{i=0}^{m-1} \beta^{2^i} = (a_{m-1}, a_0, \ldots, a_{m-2})$$

가 된다. F_{2^m} 상에 Normal basis 표현을 하면 제곱 연산이 벡터 표현 값의 단순 회전이고 1 클럭 사이클만이 하드웨어로 요구되므로 구현에 장점이 있다.

Normal basis의 곱셈은 다소 복잡하다. $A = (a_0, a_1, \ldots, a_{m-1}), B = (b_0, b_1, \ldots, b_{m-1})$이 F_{2^m} 상에 임의의 원소라 하자. $C = A \cdot B = (c_0, c_1, \ldots, c_{m-1})$ 이라 놓으면

$$C \;=\; \sum_{k=0}^{m-1} c_k\beta^{2^k} \tag{6.1}$$

이 된다.

만일

$$\beta^{2^i}\beta^{2^j} \;=\; \sum_{k=0}^{m-1} \lambda_{ij}^{(k)}\beta^{2^k}, \lambda_{ij}^{(k)} \in \{0,1\} \tag{6.2}$$

이면 식(6.1)에 β^{2^k}의 계수를 비교하면

$$c_k \;=\; \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \lambda_{ij}^{(k)}, 0 \le k \le m-1 \tag{6.3}$$

식을 얻는다. 식(6.2)의 양변에 2^{-l} 승을 하면

$$\beta^{2^{i-l}}\beta^{2^{j-l}} \;=\; \sum_{k=0}^{m-1} \lambda_{i-l,j-l}^{(k)}\beta^{2^k} = \sum_{k=0}^{m-1} \lambda_{ij}^{(k)}\beta^{2^{k-l}} \tag{6.4}$$

가 된다. 식(6.4)에서 β^{2^0}의 계수를 같게 하면,

$$\lambda_{ij}^{(l)} = \lambda_{i-l,j-l}^{(0)}, \text{ for all } 0 \le i,j \le m-1$$

따라서 식(6.3)은 다음과 같이 다시 쓸 수 있다.

$$c_k = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \lambda_{i-k,j-k}^{(0)} = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{i+k} b_{j+k} \lambda_{ij}^{(0)}$$

입력이 A와 B인 논리 회로가 곱의 계산 c_0를 계산한다면, 입력 $A^{2^{-k}}$와 $B^{2^{-k}}$에 동일한 입력을 넣으면 된다. $A^{2^{-k}}$와 $B^{2^{-k}}$는 A와 B의 벡터 표현에 간단한 cyclic shift가 된다는 점을 주의하자. 이 방법으로 C는 m 회의 클럭 사이클로 연산이 가능하다. Massey와 Omura[119]는 이런 normal basis의 특징을 이용하여 serial-in serial-out 곱셉기를 구성하였다.

이런 회로의 복잡도는 C_N이라고 하면 $\lambda_{ij}^{(0)}$의 non-zero 항의 수이고, A와 B 및 C를 포함하는 레지스터 간의 연결 수이다. 분명히 $C_N \le m^2$이다. C_N의 하한치는 $C_N \ge 2m-1$[110]이다. 만일 $C_N = 2m-1$이면, normal basis는 optimal이라고 한다. ONB는 Mullin, Onyszchuk, Vanstone, Wilson [110]에 의하여 소개되었으며, 이 기저가 존재하는 체에 관한 표와 함께 구성방법도 제시하였다. 이런 구조의 하드웨어 구현은 [2]에 제시되었으며, 이 구조를 이용하면, 곱셈은 m 클럭 사이클만에 수행된다.

결국, 곱셈 수를 최소화하는 관점에서 보면 F_{2^m} 상에 역원을 계산하는 가정 효율적인 알고리즘은 Itoh, Teechai, Tsujii [59]에 의해 제안되었다. 만일 $\alpha \in F_{2^m}, \alpha \neq 0$이면

$$\alpha^{-1} = \alpha^{2^m-2} = (\alpha^{2^{m-1}-1})^2$$

이다. 만일 m이 홀수이면,

$$2^{m-1}-1 = (2^{(m-1)/2}-1)(2^{(m+1)/2}+1)$$

이므로

$$\alpha^{2^{m-1}-1} = \left(\alpha^{2^{(m-1)/2}-1}\right)^{2^{(m-1)/2}+1}$$

이다.

$\alpha^{2^{(m-1)/2}-1}$을 계산해 두었다면, (제곱에 걸리는 계산은 무시한다면) $\alpha^{2^{m-1}-1}$를 계산하는 데는 1회의 곱셈이 필요하다. 만일 m이 짝수이면,

$$2^{m-1-1} = \alpha^{2(2^{(m-2)/2}-1)(2^{(m-2)/2}+1)+1}$$

이므로 일단 $\alpha^{2(m-2)/2-1}$이 계산되었으면, 2회의 곱셈으로 $\alpha^{2^{m-1}-1}$을 계산할 수 있다. 이 과정을 재귀적으로 반복한다.

예 6.1 *$F_{2^{155}}$를 생각한다.*

$$\begin{aligned} 2^{155}-2 &= 2(2^{77}-1)(2^{77}+1) \\ 2^{77}-1 &= 2(2^{19}-1)(2^{19}+1)(2^{28}+1)+1 \\ 2^{19}-1 &= 2(2^{9}-1)(2^{9}+1)+1 \\ 2^{9}-1 &= 2(2+1)(2^{2}+1)(2^{4}+1)+1 \end{aligned}$$

그리하여 $F_{2^{155}}$ 상의 역원 계산에는 10회의 곱셈이 필요하다.

Induction에 의하여 이 방법은 정확히 $I(m) = \lfloor \log_2(m-1) \rfloor + \omega(m-1) - 1$회의 체 연산이 필요하다, 단, $\omega(m-1)$은 $(m-1)$을 2진 표현을 하였을 때 1의 개수를 의미한다.

제 2 절 곡선과 체 K의 선택

편리 상 2.4절과 2.5절에서 정의한 덧셈 공식을 인용하자.

$E : y^2 = x^3 + ax + b$ **의 덧셈 공식**
만일 $P = (x_1, y_1) \in E$ 이면 $-P = (x_1, -y_1)$이다. 만일 $Q = (x_2, y_2) \in E$, $Q \neq -P$이면 $P + Q = (x_3, y_3)$은 다음과 같다.

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

단,

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{, if } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases}$$

$E/F_{2^m} : y^2 + xy = x^3 + a_2x^2 + a_6$**의 덧셈 공식**

$P=(x_1,y_1)\in E_1$이라 하고, $-P=(x_1,y_1+x_1)$이다. 만일 $Q=(x_2,y_2)\in E_1$ 이고 $Q\neq P$이면 $P+Q=(x_3,y_3)$은 다음과 같다.

$$x_3=\begin{cases}\left(\dfrac{y_1+y_2}{x_1+x_2}\right)^2+\dfrac{y_1+y_2}{x_2+x_1}+x_1+x_2+a_2 & P\neq Q\\ \\ x_1^2+\dfrac{a_6}{x_1^2} & P=Q\end{cases}$$

그리고

$$y_3=\begin{cases}(\dfrac{y_1+y_2}{x_1+x_2})(x_1+x_3)+x_3+y_1 & P\neq Q\\ \\ x_1^2+(x_1+\dfrac{y_1}{x_1})x_3+x_3 & P=Q\end{cases}$$

$E/F_{2^m}: y^2+a_3y=x^3+a_4x+a_6$**의 덧셈 공식**
$P=(x_1,y_1)\in E_2$이라 하고, $-P=(x_1,y_1+a_3)$이다. 만일 $Q=(x_2,y_2)\in E_2$ 이고 $Q\neq P$이면 $P+Q=(x_3,y_3)$은 다음과 같다.

$$x_3=\begin{cases}(\dfrac{y_1+y_2}{x_1+x_2})^2+x_1+x_2 & P\neq Q\\ \\ \dfrac{x_1^4+a_4^2}{a_3} & P=Q\end{cases}$$

그리고

$$y_3=\begin{cases}\left(\dfrac{y_1+y_2}{x_1+x_2}\right)(x_1+x_3)+y_1+a_3 & P\neq Q\\ \\ \left(\dfrac{x_1^2+a_4}{a_3}\right)(x_1+x_3)+y_1+a_3 & P=Q\end{cases}$$

따라서, 타원 곡선 상의 덧셈은 3개의 곱셈과 기반 체 K 상에서의 1개의 역원 계산에 의하여 가능하며, 2배는 K 상에서 1회의 역원 계산과 4회의 곱셈이 필요하다.

덧셈과 뺄셈에 대하여는 상대적으로 간단하기 때문에 고려하지 아니한다. 곡선과 체 F를 2점의 덧셈에서 체 연산의 수가 최소화되도록 선정하면 된다. $K=F_{2^m}$ 상에 곡선은 다음의 4가지 이유로 우선된다.

(i) 표수가 2 이상의 유한체에서의 연산보다 F_{2^m} 상에서의 연산이 하드웨어로 쉽게 구현된다.

(ii) F_{2^m} 상에서의 ONB 표현을 이용하면, 원소의 제곱은 벡터 표현의 1회 cyclic shift와 같게 된다. 2점의 덧셈에서 곱셈의 회수가 감소된다.

(iii) F_{2^m} 상에서의 곡선을 이용하면, 주어진 x 좌표 값에 부수적인 1 비트 정보를 이용하면 y 좌표 값을 구할 수 있다. ElGamal 암호 시스템에 있어서 메시지 확장을 축소하는 데 유용하다.

(iv) 4번째 이유는 초특이 곡선에 적용된다. F_{2^m} 상에서의 초특이 곡선에 대하여 점의 2배하는 데 역원 계산은 $a_3 = 0$으로 하면 소멸되고 결국 연산 회수를 줄이게 된다.

이러한 이유로 F_{2^m} 상에서 비 초특이 곡선을 고려하게 된다. 초 특이 곡선의 구현에 대하여는 6절에서 언급하겠다.

F_q, $q = 2^m$ 상에서 비 초특이 타원 곡선의 동형 류는 $2(q-1)$개가 있으며 각 class의 대표 곡선의 집합은

$$y^2 + xy \;=\; x^3 + a_2x^2 + a_6 \tag{6.5}$$

단, $a_6 \in F_q\backslash\{0\}, a_2 \in \{0, \gamma\}$이고 γ는 trace 1의 F_q 상의 원소이다.

전술한 바가 있는 Algorithm 2에 의한 공격이 실질적이지 아니하므로, 비 초특이 타원 곡선에 대한 대수 문제를 위한 알려진 최량의 알고리즘은 baby-step giant-step 알고리즘이다. 비 초특이 타원 곡선은 위수가 큰 소수 즉, 40자리 이상의 소인수로 나누어 질 수 있도록 하여야, 암호학적 응용에 적합하다. 결국 기반 체의 크기는 최소 2^{130}이어야 한다. 기반 체는 효율적인 체 연산을 위하여 ONB를 가져야 한다. 부가하여, 곡선이 순환 군이 되어야 하고 즉, $\#E(F_q)$ 가 중복되는 소인수가 없어야 한다.

곡선의 선정 방법에는 F_q 상에 E를 선택하는 것으로 q는 충분히 적어 $\#E(F_q)$를 직접 계산 할 수 있고, 적절한 n에 대한 군 $E(F_{q^n})$을 이용한다. Weil 정리에 의하여 $\#E(F_{q^n})$는 $\#E(F_q)$로 부터 계산된다. 만일 l이 n을 나눈다면, $\#E(F_{q^l})$이 $\#E(F_{q^n})$을 나누고, n을 소수가 되도록 선정하든가, 작은 소수와 큰 소수의 곱으로 하여야 한다.

예 6.2 *$F_{2^{155}}$ 상에서 비 초특이 타원 곡선을 선정하는 데는 F_{2^5} 상에 정의된 곡선을 뽑을 수 있다. $\#E(F_{2^5})$에는 12개의 가능성이 있다. 물론, $\#E(F_{2^{155}})$가 큰*

표 6.1: F_{2^5} 상에서의 비 초특이 타원 곡선

$\#E(F_{2^5})$	$\#E(F_{2^{155}})$의 최대 소수 약수의 자리수
22	37
28	36
36	46
38	36
42	41

소수로 나누어 지는 5개의 값이 있다. 5개의 값에 대한 $\#E(F_{2^{155}})$에 대한 가장 큰 소수 divisor의 크기를 표(6.1)에 제시하였다. $\#E(F_{2^5}) = 3642$가 암호 목적에는 최적이다.

만일 랜덤한 타원 곡선 E가 필요하다면, $\#E(F_q)$는 Schoof 알고리즘 [136]에 의하면 다항식 시간에 계산된다. Koblitz에 의하여 표수 2인 경우에도 확장되었다 [71]. 다음에 이 방법의 구현을 연구한다. Koblitz는 경험적인 방법으로 E/F_q는 랜덤하게 비 초특이 타원 곡선을 선정하면 $N = \#E(F_q)$가 소인수 ($\geq N/B$)에 의하여 나누어 질 확률은 약 $\frac{1}{m}\log_2(B/2)$이다. 따라서, 예를들면, $F_{2^{155}}$ 상에 비 초특이 타원 곡선이 위수가 40 자리 소수로 나누어 질 확률은 약

$$\frac{1}{155}\log_2\left(\frac{2^{155}}{2\cdot 10^{40}}\right) \approx 0.136$$

이다.

제 3 절 투영 좌표

덧셈 공식으로 부터 $K = F_{2^m}$ 상에 비 초특이 타원 곡선의 서로다른 2개 점을 더하는 것은 2회의 체 곱셈과 1회의 역원 계산이 필요하다. F_{2^m}상에서 역원 계산에 특별한 방법이 있다하더라도, 역원 계산은 곱셈에 비하여 비용이 훨씬 많이 든다. 2 점을 더할 때 필요한 역원 계산은 투영 좌표 (projective coordinate)를 이용하면 불필요하게 된다.

E/K를 비 초특이 곡선 $y^2 + xy = x^3 + a_2x + a_6$라고 한다. 곡선 E는 동차 3차 방정식 $y^2z + xyz = x^3 + a_2x^2z + a_6z^3$을 만족하는 투영 평면 $P^2(K)$에서 모

든 점들의 집합으로 볼 수 있다. $P = (x_1 : y_1 : z_1) \in E, Q = (x_2 : y_2 : 1) \in E$이고 $P, Q \neq \mathcal{O}, P \neq Q, P \neq -Q$이라 가정한다. $P = (x_1/z_1 : y_1/z_1 : 1)$는 affine 좌표에서 E를 위한 덧셈을 사용하면 $P + Q = (x_3' : y_3' : 1)$을 다음과 같이 얻을 수 있다.

$$\begin{aligned} x_3' &= \frac{B^2}{A^2} + \frac{B}{A} + \frac{A}{z_1} + a_2, \\ y_3' &= \frac{B}{A}\left(\frac{x_1}{z_1} + x_3'\right) + x_3' + \frac{y_1}{z_1} \end{aligned}$$

단, $A = (x_2 z_1 + x_1)$, $B = (y_2 z_1 + y_1)$이다. x_3'과 y_3'의 표현식에서 분모 성분을 없애기 위하여 $z_3 = A^3 z_1, x_3 = x_3' z_3, y_3 = y_3' z_3$로 놓으면 $P + Q = (x_3 : y_3; z_3)$은 다음과 같이 된다.

$$\begin{aligned} x_3 &= AD \\ y_3 &= CD + A^2(Bx_1 + Ay_1) \\ z_3 &= A^3 z_1 \end{aligned}$$

여기서 $C = A + B$, $D = A^2(A + a_2 z_1) + z_1 BC$이다. 이 덧셈은 아핀 좌표에서는 2회의 덧셈보다 많은 13회의 곱셈이 수행된다. 그러나, 값 비싼 역 계산이 필요 없다. P와 Q의 부가 저장 레지스터가 필요하고 덧셈에서 중간 값의 저장하는 공간의 비용이 소요된다.

$2P = (x_3 : y_3 : z_3)$의 계산 공식으로는

$$\begin{aligned} x_3 &= AB \\ y_3 &= x_1^4 A + B(x_1^2 + y_1 z_1 + A) \\ z_3 &= A^3 \end{aligned}$$

여기서 $A = x_1 z_1$, $B = a_6 z_1^4 + x_1^4$이다. 2배는 7회의 곱셈으로 수행되며, 1회 역 계산과 3회 곱셈이 필요한 아핀 좌표보다 득이 있다.

k는 양정수이고, P는 아핀 점 $(x_1, y_1, 1)$이라면 곱셈 kP는 accumulator의 2배와 필요시 P와의 덧셈에 의하여 계산된다. 결과 값 $kP = (x_3, y_3, z_3)$은 각 좌표 값에 z_3^{-1}를 곱하면 아핀 좌표 값을 얻을 수 있다. 만일 $\omega(k) = t + 1$이면 kP를 계산하는 데 총 연산 수는 $13t + 7m + 2$의 체 곱셈과 1회 역 계산이다.

제 4 절 ElGamal 암호 시스템

타원 곡선 군을 이용하여 message passing을 위한 ElGamal 암호 시스템을 고찰한다.

E는 F_{2^m} 상에서의 비 초특이 타원 곡선 $y^2 + xy = x^3 + a_2x^2 + a_6$라고 하고 P는 E에 알려진 점, E의 generator라고 한다. F_{2^m}의 원소들은 normal basis에 의하여 표현되었다고 가정한다. 사용자 A는 정수 a를 랜덤하게 선택하고, 공개 점 aP를 생성하고 a는 비밀로 한다. 메시지는 F_{2^m} 상에서 원소의 순서 쌍으로 구성되었다고 가정한다. 메시지 (M_1, M_2)를 A에게 보내기 위하여 송신자 B는 랜덤 정수 k를 선택하여 kP 와 $akP = (\overline{x}, \overline{y})$를 계산한다. $\overline{x}, \overline{y} \neq 0$ ($\overline{x}$ /0 또는 $\overline{y} = 0$일 경우는 랜덤한 k에 대하여 무시할 수 있는 확률로 발생) 라고 가정하면, B는 A에게 kP점과 M_1x와 M_2y를 보낸다. 메시지를 복호하기 위하여는 A는 점 kP에 자신의 비밀 키 a를 곱하여 $(\overline{x}, \overline{y})$를 얻고, 2회의 나눗셈으로 M_1과 M_2를 복구한다.

이방법의 결점으로는 적이 우연히 M_1 (또는 M_2)를 알게 되면 M_2 (또는 M_1)를 쉽게 얻을 수 있다. 이런 공격은 $(kP, M_1\overline{x})$를 보냄으로 방지된다. ElGamal 암호 시스템에 있어서 2개의 체 원소를 가진 메시지를 전송하기 위하여는, 4개의 체 원소를 보내야 한다. 이런 것은 메시지 확장이 2배로 된 것이다. 메시지 확장은 $P = (x_1, y_1)$을 보내는 대신에 x_1과 y_1/x_1의 (만일 $x_1 \neq 0$) 한 비트를 보낸다면 3/2로 줄어 들 수 있다. 우선 만일 $x_1 = 0$이라면 $y_1 = \sqrt{a_6}$로 한다. 만일 $x_1 \neq 0$이라면 변수 변환 $(x, y) \rightarrow (x, xz)$는 식(6.5)의 곡선 방정식을 $z^2 + z = x + a_2 + a_6x^{-2}$로 변환한다. $\alpha = x_1 + a_2 + x_6x^{-2}$를 계산한다. 2차 방정식 $z^2 + z = \alpha$를 풀어서 $z = (z_0, z_1, \ldots, z_{m-1})$, $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$를 각각 z와 α의 벡터 표현이라고 하면

$$z^2 + z = (z_{m-1} + z_0, z_0 + z_1, \ldots, z_{m-2} + z_{m1-}).$$

이 된다. 각 $z_0 = 0$ 또는 $z_0 = 1$이면 $z^2 + z = \alpha$의 유일한 해 $\overline{z}$를 결정한다. 옳바른 값 $\overline{z}$는 보내진 y_1/x_1의 해당 비트와 비교하여 결정한다. 결국, y_1은 $x_1\overline{z}$로 복원된다.

만일 모든 사용자가 동일한 타원 곡선과 기저 점 P를 사용한다면, 공개키 즉, 점 aP는 $m + 1$ 비트가 된다. 그렇지 아니하면, 공개키는 a_6 (a_2는 0으로 고정 가능), 점 P와 aP로 구성되어 $3m + 2$ 비트가 된다.

제 5 절 성 능

ElGamal 공개키 암호 시스템과 유사한 타원 곡선을 이용할 때, 암호화 속도를 추정하자. 추정은 kP 계산에 의존하며, ElGamal 및 일반화한 NIST 서명 알고리즘에 적용된다. 구체화 하기 위하여 명확성을 위하여 $F_{2^{155}}$, $(m = 155)$ 상의 비 초특이 타원 곡선을 고려한다. $F_{2^{155}}$ 에서 ONB가 있으므로 이 선택은 적절하다.

$F_{2^{155}}$ 상의 곱셈은 155회 클럭 사이클이 요구된다. 반면 역 계산은 $I(155) = 10$회의 곱셈이 요구된다. 투영 좌표를 이용하면 2점의 덧셈에 13회 곱셈과 7회 2배 계산이 걸린다.

ElGamal 시스템에서 kP와 kaP의 계산에는 랜덤하게 선정된 k에 대하여 평균적으로 m회 덧셈과 $2m$회의 2배 연산이 필요하다. 시스템의 속도를 향상과 암호화의 상한을 정하기 위하여는 k의 Hamming weight를 임의의 d ($d \leq m$)로 제한한다. 유사한 기법이 RSA에 사용[55],[2] 된다. 정수 d는 $\binom{m}{d/2}$ 이 커서 square root 공격에 대비할 수 있도록 선택하여야 한다. 현재 $d = 30$으로 하자.

kP의 계산은 29회 덧셈과 155회 2배 계산, 1회 역 계산, 1회 곱셈이 필요하다. kaP의 계산에도 동일하게 소요된다. $kaP = (\overline{x}, \overline{y})$에서 $M_1\overline{x}$와 $M_2\overline{y}$의 계산에 별도로 2회의 곱셈이 필요하다. 따라서, 암호화하는 데 2950회 체 곱셈을 하여야 2개의 체 원소를 얻는다. 결국, 40MHz 클럭 속도라면, 암호화 속도로

$$\frac{310 \times 40,000,000}{1000 \times 2950 \times 155} \approx 27\text{Kbits/sec.}$$

가 된다. 만일 추가 레지스터의 이용이 가능하고, 소프트 웨어 구현일 경우 kP의 연산은 P 값의 배수를 사전 계산함으로하여 [17] 상당히 속도 향상을 할 수 있다.

제 6 절 초특이 곡선의 이용

지금까지 비 초특이 곡선에 대하여 한정한 토의를 하였다. 그러나 추특이 곡선은 구현에 상당히 매력적이다. F_2^m (odd m) 상의 초특이 곡선의 경우를 고려한다.

F_2^m (odd m) 상의 초특이 곡선은 3 종류의 동형 류가 있다. 각 분류의 대표 곡선은 다음과 같다.

$$\begin{aligned} E_1 &: y^2 + y = x^3 \\ E_2 &: y^2 + y = x^3 + x \\ E_3 &: y^2 + y = x^3 + x + 1 \end{aligned}$$

이 3개의 곡선의 k 값은 각각 2,4, 4이다. E_2와 E_3 곡선 만을 고려하자. 우리의 현재 지식으로 이 곡선의 대수 문제는 확장 체 $F_{2^{4m}}$에서 대수 문제와 동등하다. E_2와 E_3의 덧셈 공식은 다음과 같이 간단화 된다.

$$x_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2 & P \neq Q \\ \\ x_1^4 + 1 & P = Q \end{cases}$$

그리고

$$y_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + y_1 + 1 & P \neq Q \\ \\ x_1^4 + y_1^4 + 1 & P = Q \end{cases}$$

만일 normal basis 표현을 F_{2^m} 의 원소 표현에 선택하였다면, E_2 또는 E_3에서 2배는 아주 쉽다. 반면, 2점의 덧셈은 2회의 곱셈과 1회의 역 계산으로 가능하다. 점 P의 kP는 repeated square-and-multiply로 계산될 수 있다. 만일 $\omega(k) = t + 1$이라면 지수승은 $2t$의 곱셈과 t회의 역 계산이 소요된다.

2점의 덧셈에서 필요한 역 계산은 투영 좌표를 이용하면 제거된다. 공식을 계산하면, E는 E_2 또는 E_3라 하고, $P = (x_1 : y_1 : 1) \in E$), $Q = (x_2 : y_2 : z_2) \in E$이고 $P, Q \neq \mathcal{O}, P \neq Q, P \neq -Q$라고 가정한다. 그러면 $P+Q = (x_3 : y_3 : z_3)$는

$$\begin{aligned} x_3 &= A^2Bz_2 + B^4 \\ y_3 &= (1 + y_1)z_3 + A^3z_2 + AB^2x_2 \\ z_3 &= B^3z_2 \end{aligned}$$

단, $A = (y_1z_2 + y_2)$, $B = (x_1z_2 + x_2)$이다. 이 덧셈 공식은 체 원소의 9회의 곱셈이 요구된다.

이러면 repeated square-and-multiply 방법에 의거 P가 아핀 점 $(x_1, y_1, 1)$인 kP를 계산 할 수 있다. 결과 $kP = (x_3, y_3, z_3)$는 각 좌표 값을 z_3^{-1}을 곱하여 아

핀 좌표 값으로 원래 변환이 된다. 만일 $\omega(k) = t+1$이면, kP를 연산하는 총 회수는 $9t+1$ 회의 체 곱셈과 1회의 역 계산이다.

비 초특이 타원 곡선과 마찬가지로 E_2 또는 E_3를 이용하여 ElGamal 암호 시스템을 구현하는 데 이용된다. 마찬가지로 메시지 확장 계수를 kP의 x_1좌표와 kP의 y_1 좌표의 1 비트를 보냄으로 하여 3/2로 줄일 수가 있다.

y_1은 다음과 같이 이 정보로 부터 쉽게 복구된다. 우선 $\alpha = x_1^3 + x_1$ 또는 $x_1^3 + x_1 + 1$을 각각 $E = E_2$ 또는 E_3에 따라 x_1 과 x_1^2의 단순 곱셈에 의하여 계산한다.

α의 trace가 0이므로 우리는 다음의 2가지 중 하나를 얻는다.

$$\begin{aligned} y_1 &= \alpha + \alpha^{2^2} + \alpha^{2^4} + \ldots + \alpha^{2^{m-1}} \\ y_1 &= \alpha + \alpha^{2^2} + \alpha^{2^4} + \ldots + \alpha^{2^{m-1}} + 1 \end{aligned}$$

식별자 1은 all 1의 벡터로 표현된다. 그리고 y_1의 한 비트는 y_1에 대한 바른 값을 찾는 데 이용된다. y_1의 계산은 그리 비싸지는 아니하다. 왜냐하면, y_1의 계산 공식에는 각 항은 α를 연속 제곱하여 구할 수 있기 때문이다.

ElGamal 공개키 암호 시스템과 유사한 타원 곡선 암호를 이용하였을 때 암호화 속도를 추정한다. F_{2^m}에서 곱셈은 m 클럭 사이클이 필요하고 역 계산은 $I(m) = \lfloor \log_2(m-1) \rfloor + \omega(m-1) - 1$의 곱셈이 필요하다. 간단히, 체의 덧셈과 제곱은 무시한다. 타원 곡선 점은 투영 좌표에 의하여 표현된다. 시스템의 속도를 높히기 위하여 또한 암호화 시간의 상한을 두기 위하여 k의 Hamming weight는 30으로 제한한다.

kP와 kaP의 계산에는 58회 덧셈과 2회 역 계산과 4회 곱셈이 필요하다. $kaP = (\overline{x}, \overline{y})$라 하면 $M_1\overline{x}$와 $M_2\overline{y}$ 계산하는 데 또 다른 2회의 곱셈이 필요하다. 2개 체 연산은 $528 + 2I(m)$회 체 곱셈에 의하여 암호화 될 수 있다. 구체적으로 $F_{2^{239}}$ 상의 E_3라고 하자. 이 선택은 $F_{2^{239}}$에는 ONB가 존재하므로 적절하다. 또한, $\#E_3(F_{2^{239}}$는 72 자리 소수이므로 타원 곡선 대수 문제의 square root attack은 적용되지 아니한다. 결국 $I(239) = 12$임으로 클럭 속도를 40MHz라고 하면 암호화 속도는 다음과 같다.

$$\frac{478 \times 40,000,000}{1000 \times 552 \times 239} \approx 145 \text{ Kbits/sec}$$

표 (6.2)는 ONB가 존재하고 square-root attack에 방지하는 $\#E_2(F_{2^m})$ 또는 $\#E_3(F_{2^m})$이 큰 소수를 가지는 체 F_{2^m}을 정리하였다. 곡선의 위수의 소인수 분

해는 [19]로 부터 얻었다. $F_{2^{4m}}$에서 index calculus 공격의 해독 시간을 F_{2^n}상의 이산 대수 문제[115]를 푸는 데 걸리는

$$\exp\left((1.35)n^{1/3}(\ln n)^{2/3}\right)$$

의 연산을 점근적 수행 시간의 예측에 이용하여 제시하였다.

표 6.2: 홀수 m의 F_{2^m}사의 적절한 초특이 타원 곡선

m	곡선	F_{2^m} 상의 곡선의 위수	$F_{2^{4m}}$ 에서 Index calculus 방법에 의한 연산 추정치
173	E_2	$5 \cdot 136256405957 \cdot P42$	1.4×10^{18}
173	E_3	$7152893721041 \cdot P40$	1.4×10^{18}
179	E_3	$1301260549 \cdot P45$	2.5×10^{18}
191	E_2	$5 \cdot 3821 \cdot 89618875387061 \cdot P40$	8.6×10^{18}
191	E_3	$25212001 \cdot 5972216269 \cdot P41$	8.6×10^{18}
233	E_2	$5 \cdot 3108221 \cdot P63$	4.3×10^{20}
239	E_2	$5 \cdot 77852679293 \cdot P61$	7.2×10^{20}
239	E_3	$P72$	7.2×10^{20}
281	E_3	$91568909 \cdot PRP77$	2.3×10^{22}
323	E_3	$137 \cdot 953 \cdot 525313 \cdot P87$	5.3×10^{23}

제 7 절 Z_n 상의 타원 곡선 암호 시스템

이 방법을 시작하려면 각 사용자 A는 2개의 큰 소수 p와 q를 각각이 2 modulo 3이 되도록 선택하고 $n = pq$를 계산한다. 그러면 A는 $\gcd(e, (p+1)(q+1))$이 되도록 랜덤 정수 e를 선택한다. 그리고 다음과 같이 되도록 정수 d를 계산한다.

$$ed \equiv 1 \pmod{(p+1)(q+1)}$$

A는 n과 e를 공개한다. 메시지 $m = (x, y) \in Z_n \times Z_n$을 A에게 보내기 위하여 B는 군

$$\tilde{E}_{0,b}(Z_n) = E_{0,b}(F_q) \times E_{0,b}(F_q)$$

에서

$$e \cdot (x, y) = (c_1, c_2)$$

를 계산한다. 단, $b = y^2 - x^3 \pmod{n}$이다. m이 $\tilde{E}_{0,b}(Z_n)$에 있다. B는 2.8절에서 기술한 바와 같이 군 법칙의 적용이 성공하지 아니할 확률이 멀리 있으므로 $\tilde{E}_{0,b}(Z_n)$에 계산을 함으로 위의 계산을 할 수 있다. B는 다음을 계산하여 메시지를 복구하는 A에게 (c_1, c_2)를 전송한다.

$$d \cdot (c_1, c_2) = (x, y)$$

위의 방정식은 예 2.17에서 보듯이 사실이다. 왜냐하면

$$\#E_{0,b}(F_p) = p + 1 \text{ and } \#E_{0,b}(F_q) = q + 1$$

이고

$$\#\tilde{E}_{0,b}(Z_n) = (p+1)(q+1)$$

이다.

RSA와 같이 이 시스템은 A에 의하여 메시지를 서명하는 데 이용될 수 있다.

암호 시스템은 연산이 수행되는 특정 곡선이 메시지에 의존한다는 재미있는 성질이 있다. RSA 시스템과 같이 안전성은 n의 소인수분해의 어려움에 의존한다. 그러나 시스템의 해독이 n의 소인수 분해와 동치인지는 알 수 없다.

이 시스템이 RSA만큼 효과적이지는 않지만, RSA에 알려진 몇가지 공격에 대하여 강도가 있다는 장점이 있다.

상세한 내용은 원 논문[74]를 참조한다.

제 8 절 구현

1988년에 Newbridge Microsystem(주)은 캐나다의 Cryptech System (주) (현재는 Möbius Encryption Tech.(주)로 부름) 와 협동으로 $F_{2^{593}}$ 상에 산술 계산을 근거로 하여 여러가지 공개키 및 재래식 암호 시스템을 구현한 chip을 제작하였다. 체의 크기가 크므로 셀 연결 수를 줄이기 위하여 다소 느린 two-pass 곱셈 기법을 사용하였다. ([2] 또는 [130] 참조). 레지스터의 수를 줄이기 위하여 역 계산에 다소 늦은 방법이 사용되었다. 2개의 체 원소의 곱셈에는 1,300 클럭 사이클이 소요되며 역 계산에는 약 50,000 클럭 사이클이 소요된다. 클럭은 20MHz 이므로 곱셈과 역 계산이 각각 0.065ms, 2.5ms가 소요된다.

최근에는 $F_{2^{155}}$에서 산술 연산이 되는 VLSI 칩이[133] 제작되었다. 이 장치는 11,000 게이트를 요구한다. 곱셈은 156 클럭 사이클이 필요하고 역 계산은 약 3800 클럭 사이클이 요구된다. 칩의 클럭이 40 MHz이므로 곱셈과 역 계산이 각각 0.004ms, 0.095ms가 소요된다.

기저 체에서 연산을 수행하는 coprocessor를 이용하고 있다. 고속 programmable control processor로 Motorola DSP56000을 이용하여 다양한 타원 곡선 암호 시스템을 구현할 수 있다.

논문[54]에는 유한체 $F_{2^{104}}$에서 ElGamal 암호 시스템의 구현을 기술하였다. 암호화 속도는 2 Kbits/sec를 SUN-2 SPARC에서 얻었다. 공개키의 크기는 105 비트였다.

[31]에는 Crandell은 DH 키 교환 방식과 유사한 타원 곡선의 구현에 대하여 기술하였다. 타원 곡선은 유한체 F_{p^k} 상에 p가 Mersenne 소수 (또는 s 값이 작은 일반적인 형태 $2^r - s$) 정의한 타원 곡선이다. Crandell은 값이 비싼 나눗셈보다는 쉬프트와 덧셈을 이용하여 modulo p 상의 연산 방법을 제시하였다. 이 결과는 역 계산이 불필요한 타원곡선의 특징을 같이 살리면 타원곡선 연산을 대단히 효율적으로 구현할 수 있다. 이 시스템을 Fast Elliptic Encryption (FEE) 라고 하고 NeXT 컴퓨터는 자신들의 제품에 이것을 이용하였다.

제 9 절 참조 사항

최근의 논문[45]에 의하면 Gao와 Lenstra는 [110]에서 구성한 ONB는 근본적으로 모두 ONB이다는 것을 증명하였다. ONB가 존재하지 아니하는 체에 대하여는 소위 low-complexity normal base[4]라고 하는 것이 유용하다.

F_{2^m}에서 역 계산을 하는 Itoh, Teechai, Tsujii의 방법은 몇가지 중간 값을 저장하여야 하므로 하드웨어 구현에는 값이 비싸다. 중간 값을 저장하지 아니하는 역 계산 방법이 [1]에 기술되었으나 다소 느리다.

유한체에서 계산 방법에 대한 하드웨어 설계에 다른 방법은 [33],[41],[47],[138],[151]을 참조하고 책으로는 [61],[83],[89],[91]을 참조하라. 2절에서 6절의 내용은 [96]에 근거로 하고 있다.

암호 시스템을 위한 비 초특이 타원 곡선의 이용에 대하여는 Beth와 Schaefer[12]에 의해 고려되었다. Miyaji[104]는 소수 체 상에서 타원 곡선을 선정하는 방법을 제시하고 Schnorr의 디지털 서명을 스마트 카드 상의 구현이 적절함을 보였다. Morain[108]은 큰 소수 체 상에서 순환 타원 곡선을 구성 방법을 제시하였다.

암호 시스템에 적합한 소수 체 상의 타원 곡선을 선정하는 다른 방법으로 정수 상에 정의된 고정된 곡선 E를 선택한 후, $\#E(F_p)$가 소수가 되도록 p를 선택하는 방법이 있다.

Koblitz[69]는 소수 p가 변할 때, $\#E(F_p)$ 가 소수가 될 확률에 대한 예측하는 점근적 확률치를 제시하였다.

타원 곡선의 parameterization에 대한 다른 방법으로 Chudnovsky와 Chudnovsky[28]과 Mongomery[105]가 제시하였다. Morrain[107]은 타원 곡선에서 kP를 계산하는 통상의 2진 방법보다 빠른 알고리즘을 제시하는 addition-substraction chain을 제안하였다. Koyama와 Tsuruoka는 환 Z_n 상에 타원 곡선에 대하여 동일한 결과를 제안하였다.

지금까지 보듯이, 타원 곡선 암호 시스템은 키 크기가 작다. 비교를 위하여 RSA 시스템에 있어서 공개키는 정수 쌍 (e, n)으로 구성된다. e를 작게 선택한다 하더라고 n 값이 최소 512 비트 이상의 되어야 하는 유연성이 없다. (그러나, Vanstone과 Zuccherato에 의하면 [149] 임의로 결정된 부분을 갖는 n을 선정할 수 있는 방법을 제시하였다.) 유한체에서 이산의 지수승에 근거로 하는 ElGamal 암호 시스템에는 공개키의 크기 α^a는 체의 크기와 동일한 크기이다. 즉, 최소한 100 비트이다.

만일 $E : y^2 = x^3 + ax + b$가 소수체 F_p 상에 타원 곡선이라면 E의 twist는 곡선 $E' : y^2 = x^3 + au^2x + bu^3$이다. 여기서 u는 modulo p의 quadratic non-residue이다. $\#E(F_p) + \#E'(F_p) = 2p + 2$ 임을 쉽게 검증된다. E와 E'이 모두 순환군 일 때, Kaliski[63,64]는 집합 $\{0, 1, 2, \ldots, 2p + 1\}$에서 1방향 permutation을 구성하는 데 이 곡선을 이용하였다. 이 구성은 Meier와 Staffelbach [90]에 의하여 표수

2의 유한체 상의 타원 곡선으로 확정되었다.

Koblitz[73]은 작은 Hamming weight의 지수 k를 이용한다면, 비 초특이 타원 곡선 $y^2+xy=x^3+1$과 $y^2+xy=x^3+x^2+1$ 상 kP 계산에서 점의 2배는 거의 3/4는 공짜로 계산 할 수 있다고 하였다. [73]에는 F_2 상에 (각각 F_4, F_8, F_19 상에) $\#E(F_{2^n})$ (각각 $\#E(F_{4^n})$, $\#E(F_{8^n})$, $\#E(F_{16^n})$) 이 최소한 30 자리의 소인수를 가지고 있는 곡선의 list를 제시하였다. F_{q^n} 상에는 ONB가 존재하고 4 zero 이하의 (각각 2, 3, 4 zero) 임의의 string이 점의 단순한 덧셈에 의하여 취급된다. 이런 anomalous 곡선에 대한 연구는 Meier와 Staffelbach[90]에 의하여 진행 중에 있다.

[118]에는 Okamoto, Fujioka, Fujisaki는 $n=p^2q$ 인 환 Z_n 상에서 타원 곡선을 기반으로 하는 실질적인 디지털 서명 방식을 제안하였다. 이 방법은 RSA 서명 방식보다 몇 배나 빠르다.

제 7 장

F_{2^m} 상의 타원 곡선 점의 계산

1985년 Schoof는 체 F_q 상에 정의된 타원 곡선 E 에 있는 F_q-유리수 점의 수 $\#E(F_q)$를 계산하는 알고리즘을 제시하였다. 알고리즘의 수행 시간은 $O(\log^8 q)$이고 실제로는 상당한 시간이 요구된다. Buchmann과 Muller[20]은 Schoof 알고리즘에 Shank의 baby-step giant-step 알고리즘을 혼합하여 p가 27 자리의 소수인 F_p 상에 곡선의 위수를 계산할 수 있었다. 이 알고리즘은 SUN-1 SPARC-station에서 4.5 시간이 소요되었다.

위에 언급한 작업은 q가 홀수인 경우에도 적용된다. 그러나 암호학적 실용성 관점에서는 표수가 2인 체 상에서의 곡선이 더 매력적이다. [71]에는 Koblitz가 Schoof 알고리즘에 F_{2^m} 상 곡선에 적용하여, 랜덤 곡선의 암호시스템에서 안전성의 구현을 연구하였다. 특별히 underlying field가 $F^{2^{155}}$ 인 경우에 강조되었다. VLSI 장치가 $F_{2^{155}}$ 상에 구현되어 이러한 체 상에서 랜덤 타원 곡선의 연산을 수행한다. 결국, $F_{2^{155}}$ 상의 랜덤 곡선의 위수를 결정하는 것이 흥미로운 일이다.

여기서 Schoof 알고리즘과 F_{2^m}상에 임의의 타원 곡선의 점을 계수하는 경험적 방법을 동시에 제시한다. 이미 앞에서 초특이 곡선에 대한 점의 계수를 제시한바가 있다. 그래서 여기서는 비 초특이 타원 곡선에 경우만을 생각한다.

본 장의 구성은 다음과 같다. 1절에는 표수 2의 유한체 상의 타원 곡선의 적절한 성질을 고찰한다. 그리고 Schoof알고리즘의 개요를 2절에 기술한다. 3절에는 Schoof 알고리즘의 경험적 향상 방법을 제시하고 4절에는 실험 결과를 제시한다. 마지막으로 타원 곡선 상에 점의 계수 문제에 관한 최근의 연구를 조사한다.

제 1 절 기본사항

$q = 2^m$, $K = F_q$라 하자. E는 K 상에 정의된 비 초특이 타원 곡선이라고 하자. E를 정의하는 방정식은 다음의 형태를 갖는다.

$$y^2 + xy = x^3 + a_2x^2 + a_6 \tag{7.1}$$

단, $a_2 \in \{0, \gamma\}$, $ga \in K$로 trace 1인 고정된 원소, $a_6 \in K^*$ 이다. E와 $\tilde{E}$는 $y^2+xy = x^3+a_6$ 및 $y^2+xy = x^3+\gamma x+a_6$라고 한다. $\#E(K)+\#\tilde{E}(K) = 2q+2$임을 쉽게 검증된다. 지금부터 E의 형태는 다음과 같다고 가정한다.

$$y^2 + xy = x^3 + a_6, a_6 \in K^* \tag{7.2}$$

식7.1)에 의하여 주어진 비 초특이 곡선 E와 관련된 division polynomial $f_n(x) \in K[x]$를 소개한다.[71]

$$\begin{aligned} f_0 &= 0 \\ f_1 &= 1 \\ f_2 &= x \\ f_3 &= x^4 + x^3 + a_6 \\ f_4 &= x^6 + a_6x^2 \\ f_{2n+1} &= f_n^3 f_{n+2} + f_{n-1}f_{n+1}^3, n \geq 2 \\ xf_{2n} &= f_{n-1}^2 f_n f_{n+2} + f_{n-2}f_n f_{n+1}^2, n \geq 3 \end{aligned}$$

다항식 f_n은 x에 대하여 monic이고 n이 홀수이면, f_n의 차수는 $(n^2-1)/2$이다. division polynomial은 다음의 성질이 있어 $E[n]$ 상에서 연산을 하는 데 이용된다. 정리 (7.1)은 [77], 정리 (7.2)는 [71]에서 인용하였다.

정리 7.1 *$P = (\overline{x}, \overline{y}) \in E^*$이고 $n \geq 0$이라 하자. $f_n(\overline{x}) = 0$ 일 때만 $P \in E[n]$이다.*

정리 7.2 *$n \geq 2$이고 $nP \neq \mathcal{O}P = (\overline{x}, \overline{y}) \in E^*$ 라 한다. 그러면, $nP = (\overline{x}, \overline{y})$는 다음과 같다.*

$$\begin{aligned} \tilde{x} &= \overline{x} + \frac{f_{n-1}f_{n+1}}{f_n^2} \\ \tilde{y} &= \overline{x} + \overline{y} + \frac{f_{n-1}f_{n+1}}{f_n^2} + \frac{f_{n-2}f_{n+1}^2}{\overline{x}f_n^3} + (\overline{x}^2 + \overline{y})\frac{f_{n-1}f_{n+1}}{\overline{x}f_n^2} \end{aligned}$$

단, f_n는 $f_n(\overline{x})$을 의미한다.

K상에 정의된 E의 endormorphism ring 은 $\mathrm{End}_k E$라고 표기한다. 임의의 정수 m에 대하여 multiplication-by-m map $P \mapsto mP$는 E의 endormorphism이다. 따라서 $Z \subseteq \mathrm{End}_K E$이다. $\mathcal{O}$를 고정하고, (x, y)를 (x^p, x^p) 보내는 사상 $\phi \in \mathrm{End}_K E$는 E의 Frobenius map 이다. $\mathrm{End}_K E$에서 ϕ는 다음 관계를 만족한다.

$$\phi^2 - t\phi + q = 0$$

여기서 유일한 $t \in Z$는 Frobenuis endormorphism의 trace이다. 사실 $t = q + 1 - \#E(K)$이다. 만일 l이 odd prime이면 $E[l] \cong Z_l \oplus Z_l$이다. 결국, $E[l]$은 F_l 상의 벡터 공간으로 볼 수 있고 벡터 공간은 2 차원을 가지고 있다. $E[l]$에 제한된 사상 ϕ는 $E[l]$ 상에 선형 변환이고 특성 방정식으로 $\phi^2 - t\phi + q = 0$ 을 가진다.

제 2 절 Schoof 알고리즘의 개요

$K = F_q, q = 2^m$, E는 식(7.2)로 주어졌을 때, $\#E(K)$를 계산하는 Schoof 알고리즘의 개요를 설명한다. [136]의 방법은 홀수 표수의 체 상에서만 기술하였다. 짝수 q의 경우는 3절에서 기술한다.

$\#E(F_q) = q + 1 - t$이다. 수 L'을 3과 L' 간의 소수의 곱인 $\prod l > 4\sqrt{q}$가 되도록 선택한다. 각 홀수 소수 $l \le L'$ 에 대하여 $t \pmod{l}$을 계산한다. $|t| \le 2\sqrt{2}$이므로 CRT에 의하여 t를 복구할 수 있다.

$P = (\overline{x}, \overline{y}) \in E[l]^*$이고 $k \equiv q \pmod{l}, 0 \le k \le l - 1$라 한다.

$$\phi^2(P) + kP = \tau\phi(P) \tag{7.3}$$

가 되도록 정수 $\tau, 0 \le \tau l - 1$을 찾는다. $\phi^2(P) + kP = t\phi(P)$이므로 $(t - \tau)\phi(P) = \mathcal{O}$임이 유도된다. $\phi(P)$는 위수 l의 점이므로 $t \equiv \tau \pmod{l}$이다. 이 아이디어를 구현하는 데 문제는 $\overline{K}$에 있는 P의 좌표가 K의 작은 확장체에 존재하지 않을 수도 있다는 것으로 일반적으로 효율적으로 찾아지지 아니한다. $\overline{x}$가 division polynomial $f_l(x) \in K[x]$의 근이라는 것을 관찰하여 이 문제를 극복한다. 더욱이, 정리 (7.2)를 이용하면 kP와 $\tau\phi(P)$의 표현식을 구할 수 있다. 표현식의 좌표는 x와 y에 대한 유리함수이다. 그리고 $\phi^2(P)$와 kP의 덧셈에 추가로 규칙을 이용할 수 있다.

식 (7.3)을 만족하는 $P \in E[l]^*$이 존재하는 지를 검증하기 위하여, $\phi^2(P) + kP$와 $\tau\phi(P)$의 표현식 중 x 좌표를 같게 한고, 분모와 변수 y를 제거하여 방정식 $h_1(x) = 0$을 얻는다. 그리고 $H_1(x) = \gcd(h_1(x), f_l(x))$를 계산한다. 만

일 $H_1(x) = 1$이면, 식 (7.3)을 만족하는 $P \in E[l]^*$이 존재하지 않는다. 만일 $H_1(x) \neq 1$이면, $\phi^2(P) + kP = \pm\tau\phi(P)$ 인 $P \in E[l]^*$가 존재한다. 올바른 부호를 구하기 위하여 $\phi^2(P)+kP$과 $\tau\phi(P)$의 표현식에서 y 좌표를 같게 하고 분모와 변수 y를 제거하여 방정식 $h_2(x) = 0$을 얻는다. 그리고 $H_2(x) = \gcd(h_2(x), f_l(x))$를 구한다. 만일 $H_2(x) \neq 1$이면, P는 식(7.3)을 만족한다. 그렇지 아니하면, P는 $\phi^2(P) + kP = -\tau\phi(P)$를 만족한다. 모든 계산은 환 $K[x]$ 상에서 이루어 진다는 것을 주목한다.

$O(\log^8 q)$ 비트 연산의 수행시간은 다음과 같이 얻는다. $L' = O(\log q)$이다. 각 l에 대하여 식 (7.3)을 만족하는 τ를 탐색하기 위하여 modulo $f_l(x)$ 상에서 x^{q^2}와 y^{q^2}의 residue 계산에 좌우된다. ($\phi^2(P) = (x^{q^2}, y^{q^2})$임에 주의한다.) $f_l(x)$의 차수는 $O(\log^2 q)$이므로, 이 residue는 $O(\log^5 q)$의 채 연산 또는 $O(\log^7 q)$ 비트 연산에 계산된다. 만일 고속 연산 기법이 $K[x]$와 F_q 상의 곱셈이 사용되었다면 총 수행 시간이 임의의 $\epsilon > 0$에 대하여 $O(\log^{5+\epsilon} q)$ 비트 연산으로 줄어든다. 그러나, 고속 곱셈 기법은 대단히 큰 q에 대하여 실용적이므로 고전적인 곱셈 알고리즘만을 이용한다.

제 3 절 몇가지 경험사항

$K = F_q, q = 2^m$이고 곡선 E는 식(7.2)를 가지었다고 하자. $\#E(K) = q + 1 - t, |t| \leq 2\sqrt{q}$ 라고 하자. f_4의 division polynomial의 표현식에 의하여 $\#E(K) \equiv 0 \pmod 4$이다. 이것은 $x = \sqrt[4]{a_6}$가 K에서 f_4의 근이고, 식 $y^2 + xy = x^3 + a_6$는 $x = \sqrt[4]{a_6}$ 일 때 K 상에 해를 가지고 있기 때문이다. 따라서 $E(K)$는 위수 4의 점을 가지고 있고 $t \pmod 4$를 쉽게 결정이 된다.

다음에는 l이 odd prime 인 경우, $t \pmod l$을 찾는 방법을 기술한다.

3.1 만일 존재한다면 ϕ의 eigenvalue 탐색

ϕ를 $E[l]$상에 선형 변환이라고 하면, ϕ의 특성 방정식은 $\phi^2 - t\phi + q = 0$ 이다. $t^2 - 4q$가 mod l 상에 quadratic residue가 되든가, $t^2 - 4q$가 mod l 상에 0이 될 때에만 ϕ는 F_l 상에서 eigenvalue를 갖는다. 만일 s가 ϕ의 eigenvalue이라면, s에 해당되는 eigenspace는 집합 $\{P \in E[l] : \phi(P) = sP\}$에 해당된다. s, r이 F_l상에 ϕ의 eigenvalue이면 다음의 2가지 관찰이 유용하다.

- $s^2 - ts + q = 0$이므로 $t \equiv s + q/s \pmod l$을 얻는다.

- 만일 $s \neq r$이면, S를 s에 해당하는 1 차원 eigenspace에서 non-zero 점들의 x 좌표의 집합이라고 표기한다. 만일 $\phi(P) = sP$이면, $\phi(\phi(P)) = s\phi(P)$이다. 즉, 만일 $\alpha \in S$이면, $\alpha^q \in S$이다. $f(x) = \prod_{\alpha \in S}(x - \alpha)$는 $K[x]$상에 $f_l(x)$의 $(l-1)/2$차의 인수이다는 사실을 알 수 있다.

ω 가 정수이고 $1 \leq w \leq (l-1)/2$라 한다. $\pm\omega$가 ϕ의 eigenvalue임을 검증하기 위하여 $\phi(P) = \pm\omega P$에서 $P = (x, y) \in E[l]^*$이 존재하는 가를 점검한다. 구체적으로 $\phi(P)$와 $\pm\omega P$의 x 좌표를 같게 하면,

$$x^q = x + \frac{f_{\omega-1}f_{\omega+1}}{f_\omega^2}$$

를 얻는다. 다음과 같으면 탐색이 성공한다.

$$g_1(x) \;=\; \gcd((x^q + x)f_\omega^2 + f_{\omega-1}f_{\omega+1}, f_l) \neq 1 \tag{7.4}$$

이 계산에서 주된 단계는 $x^q \pmod{f_l(x)}$의 계산이다.

만일 $g_1(x) \neq 1$이면, $\phi(P) = \omega P$ 또는 $\phi(P) = -\omega P$인지를 확인할 필요가 있다. 만일 ϕ의 eigenvalue가 ω 와 $-\omega$이면, $t \equiv 0 \pmod{l}$이다. 이것은 $g_1(x)$의 차수가 $l-1$이면 검출된다. 그렇지 아니하면, ω 또는 $-\omega$ (또는 2 모두) 가 F_l 상에 ϕ의 2개 eigenvalue 중 하나 일 때에만 $g_1(x)$의 차수가 $(l-1)/2$이다. 다음 계산에서 x의 모든 다항식은 modulo $g_1(x)$ 로 줄여들여 있다. $\phi(P)$와 $-\omega P$의 y축을 같게 하고 분모를 없애면 다음의 방정식을 얻는다.

$$h(x, y) \;=\; xf_\omega^3(y + y^q) + f_{\omega-2}f_{\omega+1}^2 + (x^2 + y)f_{\omega-1}f_\omega f_{\omega+1} = 0 \tag{7.5}$$

$y^2 = x^3 + a_6 + xy$ 이므로 y^q의 계산에는 y^2를 연속 제곱하여 계산된다. $m-1$회의 제곱하면

$$y^q = a(x) + b(x)y$$

를 얻는다. 단, $a(x)$와 $b(x)$는 modulo $g_1(x)$에 축약된다. 식 (7.5)는 다음과 같이 된다.

$$\overline{a}(x) + \overline{b}(x)y = 0$$

$y = \overline{a}(x)/\overline{b}(x)$를 곡선 방정식 (7.2)에 삽입하면 다음의 방정식을 얻는다.

$$\overline{h}(x) = \overline{a}(x)^2 + \overline{a}(x)\overline{b}(x)x + (x^3 + a_6)\overline{b}(x)^2 = 0$$

결국, 만일 $\gcd(\overline{h}(x), g_1(x)) = 1$이면 $t \equiv \omega + q/\omega \pmod{l}$ 을 얻고 그렇지 아니하면 $t \equiv -\omega - q/\omega \pmod{l}$ 을 얻는다. ϕ의 eigenvalue 탐색 방법은 q의 odd prime power에 쉽게 확장된다.

3.2 Schoof 알고리즘

만일 F_l 상에 ϕ의 eigenvalue가 없다면, 즉, $t^2 - 4q$가 quadratic non-residue mod l이라면 τ를 식(7.3)을 만족하는 지를 Schoof test를 할 수 있다.

만일 k가 q modulo l이고 $\phi^2(P) = \pm kP$인 $P = (x, y) \in E[l]^*$이 존재한다면, 다음과 같은 경우이다.

$$\gcd((x^{q^2} + x)f_k^2 + f_{k-1}f_{k+1}, f_l) \neq 1$$

만일 $t \equiv 0 \pmod{l}$ 이면 $\phi^2(P) = -kP$이다. 그리고 만일 $\phi^2(P) = kP$이면 $\phi(P) = (2k/t)P$이다. 여기서 ϕ는 F_l에서 eigenvalue를 가지고 있다. 그러나, $t^2 - 4q$는 quadratic non-residue mod l이므로 $\phi^2(P) = -kP$라고 할 수 있다. 이로서 $t\phi(P) = \mathcal{O}$와 $t \equiv 0 \pmod{l}$이 된다.

만일 $\phi^2(P) = \pm kP$인 $P \in E[l]^*$이 없다고 가정한다. $t \pmod{l}$을 결정하기 위하여, 각 $\tau, 1 \leq \tau \leq l-1$에 대하여 식 (7.3)을 만족하는 $P \in E[l]^*$임을 검사한다. $\phi^2(P) \neq \pm kP$이므로 서로 다른 2점의 덧셈 규칙을 이용하여 $\phi^2(P) + kP$의 식을 계산한다. 구체적으로는 $(P)_x$를 점 P의 x 좌표를 나타낸다고 하자. 그러면 $k \geq 2$에 대하여

$$(\pm\tau\phi(P))_x = x^q + \frac{f_{\tau-1}^q f_{\tau+1}^q}{f_\tau^{2q}} \tag{7.6}$$

그리고

$$(\phi^2(P) + kP)_x = x^{q^2} + x + \frac{f_{k-1}f_{k+1}}{f_k^2} + \lambda^2 + \lambda$$

이다. 단,

$$\lambda = \frac{(y^{q^2} + y + x)xf_k^3 + f_{k-2}f_{k+1}^2 + (x^2 + x + y)(f_{k-1}f_k f_{k+1})}{xf_k^3(x + x^{q^2} + xf_{k-1}f_k f_{k+1}} \tag{7.7}$$

이다. 유사한 방정식을 $k = 1$인 경우에 얻을 수 있다. $\phi^2(P) + kP$와 $\pm\tau\phi(P)$의 x 좌표를 같게하고 분모와 변수 y를 없애고 $h_3(x) = 0$을 얻는다. 그러면, $h_4(x) = \gcd(h_3(x), f_l(x)) \neq 1$이면 $\phi^2(P) + kP = \pm\tau\phi(P)$인 $P \in E[l]^*$이 존재한다. 이것을 각 $\tau, 1 \leq \tau(l-1)/2$에 대하여 $\tau^2 - 4q$가 quadratic non-residue mod l 인지를 반복한다. 만일 gcd가 non-trivial 하면 $\phi^2(P) + kP$와 $\tau\phi(P)$의 y 좌표를 우선 같게 하여 올바른 부호를 결정할 수 있다. 구체적으로 $\tau \geq 2$에 대하여

$$(\tau\phi(P))_y = x^q + y^q + \frac{f_{\tau-1}^q f_{\tau+1}^q}{f_\tau^{2q}} + \frac{f_{\tau-2}^q f_{\tau+1}^{2q}}{x^q f_\tau^{3q}} + (x^{2q} + y^q)\frac{f_{\tau-1}^q f_{\tau+1}^q}{x^q f_\tau^{2q}} \tag{7.8}$$

그리고

$$(\phi^2(P) + kP)_y = \lambda(x^{q^2} + x_3) + x_3 + y^{q^2}$$

이고 $x_3 = (\phi^2(P) + kP)_x$이고 λ는 식(7.7)과 같다. (유사한 방정식은 $\tau = 1$ 인 경우에 구할 수 있다.) 위에서 한 것과 마찬가지로, 분모와 변수 y를 제거하고 $h_5(x) = 0$을 얻는다. 만일 $\gcd(f_l(x), h_5(x)) \neq 1$이면 $t = \tau$를 얻고 그렇지 아니하면, $t = -\tau$를 얻는다. 이 계산의 주된 단계는 x^{q^2}와 y^{q^2}의 계산에 있다.

실질적으로 $t \pmod{l}$을 계산하는 데는 F_l에서 eigenvalue를 우선적으로 찾아야 한다. 만일 실패하면, Schoof 알고리즘을 적용한다. 첫 번째 방법이 $x^q \pmod{f_l(x)}$의 residue를 필요로 하므로 더 빠르다. 두 번째 방법은 $x^q, x^{q^2}, y^q, y^{q^2} \pmod{f_l(x)}$의 residue가 필요하다. 경험적으로 랜덤 곡선에 대하여 ϕ는 모든 l의 반에 대하여 F_l에 eigenvalue (즉, $t^2 - 4q$가 F_l상에 quadratic residue이다)를 갖는 것을 기대한다. 더욱이 ϕ가 F_l 상에서 eigenvalue를 가지었다면, 대부분의 경우 eigenvalue는 서로 다를 것이다. 그래서 전술한 바가 있는 $\phi(P) = \omega P$ 또는 $\phi(P) = -\omega P$의 검사는 무시할 수 있는 시간이 소요된다. (왜냐하면 $\deg g_l(x) = (l-1)/2$ 또는 $l - 1$ 이다)

3.3 $t \pmod{l = 2^c}$의 결정

만일 $l = 2^c$ 이라면 $f_l(x)$가 작은 차수의 인수를 가지고 있다는 사실이 있다.

보조정리 7.1 *만일 $l = 2^c$이면 $f_l(x)$는 $K[x]$에 차수 $l/4$의 인수 $f(x)$를 가진다.*

Proof: $E[l] \cong Z_l$이므로 $f_l(x)$는 $l/2$개의 서로 다른 근을 가지고 있다. 이 중에 $l/4$는 위수 l의 점의 x 좌표이다. 따라서 $f_l(x)$는 $K[x]$에서 차수 $l/4$의 인수 $f(x)$를 갖는다. 근은 정확히 위수 l의 점의 x 좌표이다. □

다음은 인수 $f(x)$가 쉽게 구성될 수 있는 방법을 보여 준다.

보조정리 7.2 *$l = 2^c$라 하자. $K[x]$에서 다항식 $\{g_i(x)\}$의 수열은 다음과 같이 정의하자.*

$$\begin{aligned} g_0 &= x \\ g_1 &= b_1 + x \ \textit{where}\ a_6 = b_1^4 \\ g_i &= g_{i-1}^2 + b_i x \prod_{j=1}^{i-2} g_j^2, \ \textit{where}\ a_6 = b_i^{2^{i+1}}, \ \textit{for}\ i \geq 2 \end{aligned}$$

그러면 $f(x) = g_{c-1}(x)$는 $K[x]$ 상에 차수 $l/4$의 $f_l(x)$ 인수를 가지고 있다. 더욱이, $f(x)$의 근은 위수 l의 점의 x 좌표이다.

Proof: $K[x]$상에 다항식 $\{h_i(x)\}$의 수열을

$$h_0 = 1, h_1 = x, h_i = x\prod_{j=1}^{i} g_j^2 \text{ for } i \geq 2$$

로 정의하자. $P = (x, y) \in E^*$, $(2^n P)_x = G_n/H_n$, $n \geq 0$로 하자. 점의 2배수 계산 공식에 의하여 G_n과 H_n은 $K[x]$에 있어서 다항식이라는 것을 알 수 있다. Induction 방법에 의하여 $G_n = (g_n)^{2^{n+1}}, H_n = (h_n)^{2^n}, n \geq 1$에 을 증명한다. $n = 1$ 에 대하여

$$\frac{G_1}{H_1} = \frac{g_1^4}{h_1^2} = \frac{(b_1 + x)^4}{x^2} = \frac{a_6}{x^2} + x^2$$

이것이 $(2P)_x$이다. $n = i$에 사실이라고 가정하면

$$\begin{aligned}(2^{i+1}P)_x &= \frac{G_{i+1}}{H_{i+1}} = (2^i P + 2^i P)_x = \frac{a_6 H_i^2}{G_i^2} + \frac{G_i^2}{H_i^2} \\ &= \frac{(b_1 H_i + G_i)^4}{G_i H_i)^2} = \frac{(b_{i+1}h_i + g_i^2)^{2^{i+2}}}{(g_i^2 h_i)^{2^{i+1}}} = \frac{(g_{i+1})^{2^{i+2}}}{(h_{i+1})^{2^{i+1}}}\end{aligned}$$

또한, $\deg g_n = 2^{n-1}$, $n \geq 1$이 되는 것도 Induction 방법에 의하여 쉽게 증명된다.

그러면 $P \in (\overline{x}, \overline{y}) \in E^*$로 하자. $(2^{c-1}P)_x = (g_{c-1})^{2^c}/(h_{c-1})^{2^{c-1}}$이므로 $g_{c-1}(\overline{x}) = 0$과 $g_i(\overline{x}) \neq 0$ $0 \leq i \leq c-2$ 일 때만 $\mathrm{ord}(P) = 2^c$ 이다. 그러나, $h_{c-1} = g_0 \prod_{j=1}^{c-2} g_j^2$와 $\gcd(g_{c-1}, h_{c-1} = 1$이므로 $g_{c-1}(\overline{x}) = 0$ 일 때에만 $\mathrm{ord}(P) = 2^c$이다. 결국, $\deg g_{c-1} = l/4$ 이므로 원하는 인수 $f(x)$는 $g_{c-1}(x)$이어야 한다. □

q를 나누는 $l = 2^c$에 대하여 $q \equiv 0 \pmod{l}$을 얻는다. $P \in E[l]^*$에 대하여 $\phi^2(P) - \tau\phi(O) = \mathcal{O}$라는 것을 알고 있다. ϕ가 Frobenius endormorphism이므로 $P \neq \mathcal{O}$에 대하여 $\phi(P) \neq \mathcal{O}$ 이다. 그러므로 $\phi(P) - \tau P = \mathcal{O}$이고 τ는 Z_l 상에 ϕ의 eigenvalue가 된다.

$\#E(F_q) \equiv 0 \pmod{4}$를 알고 있으므로 $t \equiv 1 \pmod{4}$와 $\tau \equiv 1 \pmod{4}$이다. 이것은 τ modulo 8에 대하여 2 가지 가능한 값을 가진다. 이러한 eigenvalue는 전술한 $f_8(x)$의 인수와 eigenvalue를 찾는 경험적인 사실을 이용하여 쉽게 구할 수 있다. 이 과정을 $l = 16, 32, 64, \ldots$의 eigenvalue 계산에 유사하게 적용된다. 이 방법은 l이 2의 작은 지수승인 경우에 효율적이다. 왜냐하면 다항식 연산이 $f_l(x)$의 차수 $l/4$ 인 인수의 modulo상에서 이루어 지기 때문이다.

3.4 Baby-step Giant-step 알고리즘

작은 소수들인 l에 대한 Schoof 알고리즘을 이용한 $t \pmod{l}$의 계산은 간단하다. 그러나 $\deg(f_l(x)) = (l^2-1)/2$ 이므로 l 값이 증가할 때 계산은 상당히 어려워 진다. [20]에는 Schoof 알고리즘과 Baby-step giant-step 알고리즘을 혼합하였다. 이 방법은 우선 $\#E(F_q) \pmod{L = l_0 \cdot l_1 \cdots l_r}$ 을 계산한다. 단, $l_1, \ldots, l_r$은 작은 소수이고 l_0는 2의 작은 지수승이다. 그러면 $\#E(F_q)$의 결정에 baby-step giant-step을 사용할 수 있다.

Schoof알고리즘에 Shank 알고리즘을 변형하여 적용한다.

Step 1. $E(F_q)$ 상에 점 P를 선택하고

$$k = \min\{k' | k' \geq \left\lceil \sqrt{L \cdot 4 \cdot \sqrt{q}} \right\rceil, k' \equiv 0 \pmod{L}\}$$

로 한다.

Step 2. $1 \leq i \leq k-1$에 대하여 $i \equiv (\lfloor q+1-2\sqrt{2} \rfloor - \#E(F_q)) \pmod{L}$에 iP를 계산한다. 어떤 i에 대하여 $iP = \mathcal{O}$이면 Step 1으로 돌아간다. 그렇지 아니하면 i와 iP의 x 좌표의 첫 번째 32 비트를 iP의 값에 의해 정열하여 표에 저장한다.

Step 3. $Q = kP$로 한다.

Step 4. $j = 1, 2, \ldots, k/L$에

$$H_k = \lfloor q+1-2\sqrt{q} \rfloor P + iQ$$

를 계산하고, 어떤 i에 대하여 이진 탐색에 의하여 iP의 x 좌표 중 첫 번째 32 비트와 H_j의 x 좌표 중 첫 번째 32 비트와 같은 지를 비교한다. 만일 맞다면 $H_j = iP$ (iP를 재 계산하여)인지를 검사한다. 만일 $H_j = iP$인 한 쌍 (i, j)를 가진다면,

$$\#E(F_q) = \lfloor q+1-2\sqrt{q} \rfloor + kj - i$$

로 알고리즘을 종료하고 그렇지 아니하면 Step 1으로 돌아간다.

이 알고리즘의 정당성과 수행 시간은 다음과 같다.

$P \in E(F_q)$이므로 $\mathrm{ord}(P)$는 $\#E(F_q)$를 나눈다. 만일 유일한 정수 $r \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$가 있어 $rP = \mathcal{O}$이고 $r = \#E(F_q)$이다. 그렇지 아니하면,

$\mathrm{ord}(P) \le 4\sqrt{q}$이다. 어떠한 경우도 Step 4에서 검출되고 $\mathrm{ord}(P) > 4\sqrt{q}$를 희망한다.

$E(F_q) \cong Z_{n_1} \oplus Z_{n_2}$이고 $n_2|n_1$, $n_2|(q-1)$이다. 랜덤한 타원 곡선에 대하여 $n_1 >> n_2$ 로 기대된다. 그래서 $n_1 >> 4\sqrt{q}$ 이다. 대단히 높은 확률로 $\mathrm{ord}(P) > 4\sqrt{q}$이다. $\#E(F_q) \ge (\sqrt{q}-1)^2$ 이므로 $n_1 \ge \sqrt{q}-1$ 이다. 더욱이 $4|\#E(F_q)$ 이고 n_2가 홀수이므로, $n_1 \ge 2(\sqrt{q}-1)$이다. 사실 $n_1 \le 4\sqrt{q}$이므로 $E(F_q)$에는 위수가 $4\sqrt{q}$ 보다 큰 점은 없다. 매번 Step 4에서 실패할 것이므로 이 경우도 검출된다. 만일 이런 일이 생기면, $\mathrm{ord}(P)$를 결정하고 점 P가 $\mathrm{ord}(P) \ge 2(\sqrt{q}-1)$ 일 때까지 알고리즘을 반복한다. quotient group $E_(F_q)/ < P >$에서 위수 ≥ 3인 점 P'을 탐색한다.

Step 2에서 표는 $S = 2q^{1/2}/\sqrt{L}$개를 가지고 있고 $O(S)$ 체 연산에 의하여 계산된다. 이 표는 $O(S \log S)$의 비교로 정렬된다. $j = 1, 2, \ldots, k/L$ H_j에서 H_j를 계산하는 것은 $O(S)$ 체 연산이 필요하고 각 2진 탐색에는 $O(\log S)$ 비교가 필요하다. 따라서 총 알고리즘은 $O(q^{1/4}(\log q)^2/\sqrt{L})$ 비트 연산과 $O(q^{1/4}(\log q)/\sqrt{L})$ 비트 공간이 필요하다.

3.5 결과 검사

$\#E(F_q) = q+1-t$ 로하고 t가 미지수이다. 알고리즘이 $\#E(F_q) = q+1-t'$을 출력한다고 가정한다. $t = t'$ 인지를 다음과 같이 검사한다.

P가 baby-step giant-step 알고리즘의 점이라고 한다. 알고리즘이 종료되었으므로 $\mathrm{ord}(P) > 4\sqrt{q}$라고 믿는다. 우선 $(q+1-t')P = \mathcal{O}$를 검정하고 만일 성립하지 아니하면, $t \ne t'$이다. 그리고 $q+1-t'$을 소인수 분해를 하는 데 관심있는 q에 대하여 $q+1-t' \le 10^{50}$이므로 쉬운 일이다. $q+1-t'$의 소인수 분해가 주어지면 보조정리 (5.3)에 의하여 $\mathrm{ord}(P)$는 쉽게 결정할 수 있다. 그리하여 $(q+1-t)P = \mathcal{O}$ 과 $(q+1-t')P = \mathcal{O}$이므로 $(t-t')P = \mathcal{O}$임을 유도한다. 결국, $\mathrm{ord}(P) > 4\sqrt{q}$이고 $|t-t'| \le 4\sqrt{q}$이므로 $t = t'$으로 결론을 낸다. 물론 이 검사는 $n_1 > 4\sqrt{q}$이어야 만 성공하고 앞에서 기술한 바와 같이 대부분의 곡선에 대하여 이것은 사실이다.

제 4 절 구현과 결과

[97]에는 3절에서 기술한 알고리즘을 주 메모리 64 MB를 가진 SUN-2 SPARC-station에서 C 언어로 구현하였다. 이 구현에 대하여 몇가지 언급한다.

(i) $F_q = F_{2^m}$의 원소는 ONB로 표현된다.

(ii) $n = \deg f_l(x)$라 하자. 임의의 $A(x) \in K[x]$에 대하여 $\gcd(A(x), f_l(x))$를 계산을 위하여 $A(x)$는 modulo $f_l(x)$로 우선 줄인다. 예를 들면 식 (7.4)에서처럼 필요한 계산 $x^q \pmod{f_l(x)}$를 계산하기 위하여 $j \le j \le n-1$에 대하여 residue $x^{2^j} \pmod{f_l(x)}$를 사전 계산한다. 그러면 $x^q \pmod{f_l(x)}$는 x의 반복 제곱에 의하여 계산된다. 구체적으로

$$\begin{aligned} x^{2^i} \pmod{f_l(x)} &= \left(x^{2^{i-1}} \pmod{f_l(x)}\right)^2 \pmod{f_l(x)} \\ &= \left(\sum_{j=0}^{n-1} a_j x^j\right)^2 \pmod{f_l(x)} \\ &= \sum_{j=0}^{n-1} a_j^2 (x^{2j} \pmod{f_l(x)}) \end{aligned}$$

$x^{q^2}, y^q, y^{q^2} \pmod{f_l(x)}$의 residue도 유사하게 얻어진다.

(iii) 식(7.6)과 (7.8)을 계산하는 데는 $0 \le \tau \le (l-1)/2+1$에 $f_\tau^q \pmod{f_l(x)}$를 계산할 필요가 있다. 우리는 이미 $x^q \pmod{f_l(x)}$를 알고 있으므로 $f_\tau^q \pmod{f_l(x)}$는 재귀적으로 쉽게 계산된다.

$$\begin{aligned} f_0^q &= 0 \pmod{f_l(x)} \\ f_1^q &= 1 \pmod{f_l(x)} \\ f_2^q &= x^q \pmod{f_l(x)} \\ f_3^q &= x^{4q} + x^{3q} + a_6 \pmod{f_l(x)} \\ f_4^q &= x^{6q} + a_6 x^{2q} \pmod{f_l(x)} \\ f_{2i+1}^q &= f_i^{3q} f_{i+2}^q + f_{i-1}^q f_{i+1}^{3q} \pmod{f_l(x)}. i \ge 2 \\ f_{2i}^q &= s(x)(f_{i-1}^{2q} f_i^q f_{i+2}^q + f_{i-2}^q f_i^q f_{i+2}^{2q} \pmod{f_l(x)}. i \ge 3 \end{aligned}$$

이고 $s(x) \in K[x]$ 는

$$s(x) x^q \equiv 1 \pmod{f_l(x)}$$

을 만족한다. l이 홀수이면 $\gcd(x^q, f_l(x)) = 1$이 되고 x좌표값이 0이되는 점은 위수가 2이다.

(iv) 31까지 l을 선택하여 이 방법의 baby-step giant step에서 탐색 공간이 취급될 수 있는 크기로 유지하였다. 만일 메모리가 더 가용한다면 $l = 29$ 또는 $l = 31$인 경우는 제외하여 baby-step giant-step 에서의 탐색 시간을 증가하는 비용을 부담하면 된다. 앞에서의 방법을 이용하면 t modulo 64는 계산된다. 만일 (t modulo 64) ≤ 31이면 t modulo 128도 계산된다. (이 경우 $f_{128}(x)$의 32차 인수를 modulo로 하는 $1 \leq I \leq 31$인 division polynomial $f_i(x)$에 한함) 유사하게 만일 (t modulo 128) ≤ 31이면, t modulo 256이 계산된다. 이 방법으로 t modulo 128도 계산된다.

표 (4)에는 $F_{2^{155}}$ 상에 단일의 랜덤 곡선에 점을 계산하는 전술한 알고리즘의 주요 수행 시간을 정리하였다. 기대한 바와 같이, $x^q (\mathrm{mod}\, f_l)$가 eigenvalue를 찾기위한 주된 단계이고 x^{q^2}, y^q, y^{q^2} modulo f_l이 알고리즘의 Schoof 부분으로 주된 단계이다. 만일 eigenvalue가 존재하면, 부호를 결정하는 시간은 무시될 정도의 시간이 소요된다. eigenvalue를 찾는 것이 유용한 핵심이므로, 그러한 eigenvalue가 존재하면 상당한 시간을 절약할 수 있다. division polynomial 과 t modulo 128의 계산 시간도 무시할 수 있는 정도이다.

표 (7.2)에는 여러 가지 문제 경우에 baby-step giant-step의 시간을 정리하였다. 탐색 공간의 크기는 $4\sqrt{q}/L$이다. L은 t modulo l이 알려졌을 때 l들의 곱을 의미한다.

마지막으로 표 (7.3)은 하나의 랜덤하게 선택된 곡선과 몇가지 m 값에 대하여 $\#E(F_{2^m})$을 계산하는 방법의 총 수행 시간을 제시한다. 고정된 m에 대하여 $\#E(F_{2^m})$을 계수하는 총 수행 시간은 큰 편차를 가지고 있고, 큰 소수 l이 사용되고 F_l에 ϕ의 eigenvalue가 존재하지 아니할 때 가장 긴 시간이 관측되었다.

$\#E(F_{2^{155}})$의 계산에는 SUN-2 SPARC-station에는 약 61시간이 소요된다. (알고리즘은 ϕ가 F_{29} 또는 F_{31}에서 eigenvalue를 가진다는 조건에는 61 시간 이하가 소요된다. 경험적으로 랜덤 곡선에 대하여는 약 75 % 의 시간이 예상된다.) SPARC-station에서 $F_{2^{155}}$에서 체 요소는 초당 900회 곱셈의 비율로 곱해진다. $F_{2^{155}}$에서 체 연산을 수행하는 특별한 목적의 Chip은 초당 250,000회 곱셈을 수행한다. 알고리즘의 총 시간 중 약 90 % 는 F_{2^m}에서 체 요소의 곱셈에 사용되고 이런 chip을 사용하면 $\#E(F_{2^{155}})$의 소요 시간을 약 6시간으로 줄일 수 있다.

표 7.1: $F_{2^{155}}$ 상에 단일의 랜덤 곡선에 점을 계산하는 알고리즘의 주요 수행 시간(초)

$f_i(x), 0 \le i \le 31$의 계산시간						245.3				
t modulo 128의 계산시간						162.				
l	3	5	7	11	13	17	19	23	29	31
(a)	1.7	9.4	35.6	278	469	1231	2149	4612	11939	14170
(b)	0.1	0.7	1.1	31	69	89	458	1243	778	5252
(c)	-	-	13.1	-	-	88	-	-	72	-
(d)	1.7	9.7	-	247	488	-	2268	4890	-	15188
(e)	11.5	-	-	552	1026	-	4539	9525	-	28869
(f)	3.4	-	-	495	977	-	4539	9805	-	30141
(g)	0.1	-	-	87	299	-	2036	6072	-	22463
(h)	0.7	-	-	173	177	-	2018	786	-	6298
(i)	0.9	-	-	213	348	-	1831	3444	-	9971

기호
ϕ의 eigenvalue를 탐색
(a) $x^q \pmod{f_l(x)}$의 계산
(b) eigenvalue의 탐색
(c) eigenvalue의 부호 결정
Schoof 알고리즘
(d) $x^{q^2} \pmod{f_l(x)}$의 계산
(e) $y^q \pmod{f_l(x)}$의 계산
(f) $y^{q^2} \pmod{f_l(x)}$의 계산
(g) $f_i^q \pmod{f_l(x)}, 0 \le i \le (l-1)/2+1$의 계산
(h) $\tau, 1 \le \tau \le (l-1)/2$의 탐색
(i) τ 의 부호 결정

표 7.2: F_{2^m} 상의 곡선에 대한 baby-step giant step 부분의 소요 시간

m	step 1,2,3에 사용된 l들	탐색 공간의 크기	시간
33	3,5,64	$3.9 \cdot 10^2$	0.2 sec
52	3,5,7,11,128	$1.8 \cdot 10^3$	0.5 sec
65	3,5,7,11,13,64	$2.5 \cdot 10^4$	1 sec
82	3,5,7,11,13,17,64	$5.4 \cdot 10^5$	4 sec
100	3,5,7,11,13,17,64	$2.8 \cdot 10^8$	1min 43sec
113	3,5,7,11,13,17,64	$2.5 \cdot 10^{10}$	18min 31sec
135	3,5,7,11,13,17,19,23,64	$1.2 \cdot 10^{11}$	51min 22sec
148	3,5,7,11,13,17,19,23,29,64	$3.6 \cdot 10^{11}$	100min 42sec
155	3,5,7,11,13,17,19,23,29,31,128	$6.7 \cdot 10^{10}$	44min 11sec

표 7.3: F_{2^m} 상에 랜덤하게 선택된 곡선에 대하여 점의 계수에 총 시간

m	F_l에서 ϕ 의 eigenvalue를 가진 l	3절에서의 총 수행 시간
33	3	1min 6sec
52	3,5,7	4min 51sec
65	5	22min 29sec
82	3,7,11,13	57min 46sec
100	5,7,11,17	46min 21sec
113	3,7,17	1hr 8min 7sec
135	3,7,13,19,23	5hr 43min 47sec
148	5,7,11,13,17,19,29	16hr 7min 26sec
155	7,17,29	60hr 29min 33sec

구현되지 아니한 가능한 성능 향상은 t modulo 27의 계산에 있다. baby-step giant-step 알고리즘 대신에 kangaroo 잡는 Pollard의 Lambda 방법[123]을 이용하면 가능하다. Pollard의 방법은 baby-step giant-step 방법과 동일한 기대되는 수행 시간이 필요하나 메모리가 적게 소요된다.

제 5 절 최근 연구

$K = F_q$라 하고 3절에서 고찰한 바와 같이 ϕ가 F_l에 서로 다른 eigenvalue를 가진 소수 l 들에 대해 $K[x]$에서 $f_l(x)$의 차수 $(l-1)/2$ 인수 $f(x)$가 있다. 이런 인수가 존재하고 알려져 있다면, 상당한 시간을 절약할 수 있도록 Schoof 알고리즘에서 $f_l(x)$의 대신에 사용될 수 있다. Elkies와 Miller는 독립적으로 우선적으로 $f_l(x)$를 구성하지 아니하고, $f(x)$의 인수를 구성하는 방법을 미발간 연구 결과로 제시하였다. Charlap, Coley, Robbins[25]는 Elkies의 결과를 변형으로 $f(x)$는 어떤 한번 작업 후에 쉽게 계산될 수 있다고 제시하였다. 이 변형으로 $\#E(K)$의 계산에 $O(\log^8 q)$의 계산에서 $O(\log^6 q)$ 비트 연산으로 줄일 수 있었다. $O(\log^6 q)$의 수행 시간은 엄밀히 증명되지 아니하였다. 예를들면, $t^2 - 4q$가 모든 홀수 소수 l의 대략 반 정도에 quadratic residue module l이라는 것을 가정하였다. 이 경우는 q가 홀수 소수인 경우에만 기술되었고 $q = 2^m$의 일반적인 경우는 직접적으로 적용되지 아니하는 것 같고, 이 방법의 실질적인 구현에 대하여는 알 수 없다.

최근 Atkin[5]는 $\#E(K)$를 계산하는 새로운 알고리즘으로 modular equation을 이용하는 방법을 기술하였다. 각 홀수의 소수 l에 대하여 차수 $(l^2-1)/2$의 다항식 $f_l(x)$를 사용하는 대신에 차수 $l+1$의 다항식을 $K[x]$ 상의 modulo로 연산을 수행한다. 각 반복에는 $t \pmod{l} \in S$를 결정한다. S는 $\{0, 1, 2, \ldots, l\}$의 부분 집합으로 $|S_l| < l/2$이고 통상 $|S_l| << l/2$이다. 여러 가지 l에 대한 이런 부분 정보를 t를 계산하는 데 혼용된다. 이 알고리즘은 엄밀히 분석되지는 아니하였으나, 실제적으로 월등히 수행한다. $q \approx 10^{50}$일 잘 동작할 것 같다. Atkin는 q가 홀수 소수이고, $q \approx 10^{68}$에 $\#E(K)$를 계산하였다. 그러나 Atkin은 짝수 지표의 경우 이 방법을 변형하였다. 이 방법은 구현되었고 $\#E(F_{2^{155}})$의 계산에 9 시간으로 줄어 들었다. 그리고 $\#E(F_{2^{196}})$의 계산에 약 110 시간이 소요되었다.

최근에 Atkin[6]은 Elkies의 생각에 영향을 받아 $\#E(K)$의 새로운 계산 방법으로 modular equation을 이용하여 구현하였다. $\#E(F_q)$의 계산에 성공하였는 데 q는 홀수 소수이고 $q \approx 10^{200}$이었다. q가 짝수인 경우에 일반화는 아직까

지 적용되지 아니하는 것 같다.

제 6 절 참조 사항

이 장에서의 내용은 [97]에서 추출하였으며 AMS의 복제 허가로 재 인쇄하였다. [121]에는 Pila가 Schoof알고리즘의 일반화를 제시하였는 데 결정적 다항식 시간에 유한체 상에 정의된 abelian variety의 Frobenius endomorphism의 특성 방정식을 계산하는 방법이다. 이 경우 abelian variety는 F_q상에 정의된 대수 곡선 C의 Jacobian이고 C상에 F_q 유리수 점의 수는 쉽게 복구된다. 이 알고리즘의 구현은 아직 알 수 없다.

Cantor[23]는 타원곡선에서 division polynomial에 상응하는 것이 hyperelliptic 곡선에서 Jacobian임을 얻었다.