

ア
リ
ン
グ
ア
リ
ン
グ
の
定
義
を
整
数
と
す
る
.
 G_1, G_2
を
単
位
元
0
の
加
法
ア
ベ
ル
群
と
す
る
.
 G_1, G_2
は
位
数
 n
を
持
つ
.
 G_3
は
単
位
元
1
の
乗
法
に
関
す
る
位
数
 n
の
巡
回
群
と
す
る
.
ペ
ア
リ
ン
グ
と
い
う
の
は

2
つの
性質
を満
たす.

全
ての
 $P, P' \in$
 G_1
と
 $Q, Q' \in$
 G_2
に
対し
て,
$$e(P+P', Q)$$

$$=$$

$$e(P, Q)$$

$$+ e(P', Q),$$

$$e(P, Q+Q')$$

$$=$$

$$e(P, Q)$$

$$+ e(P, Q')$$

が
成
り
立
つ.

全
ての
 $P \in$
 $G_1 (P \neq$
 $0)$
に
対し
て
 $e(P, Q) \neq$
 1
と
な
る
よ
う
な
 $Q \in$
 G_2
が
存
在
す
る.

全
ての
 $Q \in$
 $G_2 (P \neq$
 $0)$
に
対し
て
 $e(P, Q) \neq$

$E(F_{q^m})$
 の
 位
 数
 $\#E(F_{q^m})$
 は
 $E(F_q)$
 の
 位
 数
 $\#E(F_q)$
 を
 用
 い
 て
 次
 の
 よ
 う
 に
 求
 め
 ら
 れ
 る.

$$\begin{aligned}\#E(F_{q^m}) &= q^m + 1 - t_{[m]} \\ t_{[m]} &= \alpha^m + \beta^m\end{aligned}$$

た
 だ
 し,
 t
 を
 $E(F_q)$
 の
 ト
 レ
 ー
 ス
 $t =$
 $q +$
 $1 -$
 $\#E(F_q)$
 と
 す
 る.
 こ
 の
 と
 き,
 $|t| \leq$
 $2\sqrt{q}$
 が
 成
 り
 立
 つ.
 ま
 た,
 α, β
 は
 $\alpha\beta =$
 $q, \alpha +$
 $\beta =$
 t
 を
 満
 た
 す
 複
 素
 数
 で
 あ
 る.

て, $D \sim (Q) - (O)$ となる因子 $D \in \text{Div}^0(E)$ を選択する. $\text{supp}(\text{div}(f_{n,P})) \cap \text{supp}(D) = \emptyset$ を満足するようにランダムに選んだ点 $R \in E(F_{q^k})$ を利用して $D = (Q) + (R) - (R) \in \Gamma \Gamma \Gamma \Gamma, f_{n,P}(D)$ を計算可能である. Tate ペアリングは次のように定義可能である.

$$\langle \cdot, \cdot \rangle_n : \left\{ \begin{array}{l} E(F_q)[n] \times E(F_{q^k})/nE(F_{q^k}) \rightarrow F_{q^k}^*/(F_{q^k}^*)^n \\ (P, Q) \mapsto (P, Q) \mapsto f_{n,P}(Q) \end{array} \right.$$