ペ

ペ

アリング　アリングの定義　nを整数とする.G_1, G_2を単位元0の加法アーベル群とする.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.

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

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,
$D \sim$
$(Q)-$
$(\mathcal{O})$
となる因子
$D \in$
$\mathrm{Div}^0(E)$
を選択する.
$\mathrm{supp}(\mathrm{div}(f_{n,P})) \cap$
$\mathrm{supp}(D) = /$
0
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
$D =$
$(Q+$
$R)-$
$(R)\Gamma\Gamma\Gamma\Gamma,\ f_{n,P}(D)$
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.

$$\langle \cdot, \cdot \rangle_n : \begin{cases} E(F_q)[n] \times E(F_{q^k})/nE(F_{q^k}) \to F_{q^k}^*/(F_{q^k}^*)^n \\ (P,Q) \to (P,Q) \end{cases}$$