ペアリング

ペアリングの定義

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．

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

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

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