```
ペ
アリング演算の高速化SiMAl grit第4章で述べたMAl gritでは部分群の位数 nを2進展開していたSiMAl gritは符号付き2進展開を用いる手法である次にそのアルゴリズー net re med er med re med r
```

```
Input: n, P = (x_P, y_P) \in E(F_q)[n], Q = (x_Q, y_Q) \in E(F_{q^k})

Output: f \in F_{q^k}

1: Q' \in_R E(F_{q^k})

2: S = Q + Q' \in E(F_{q^k})

3: V \leftarrow P, f \leftarrow 1, f_{-1} = \frac{1}{x_Q - x_P}

4: n = \sum_{i=0}^{l-1} n_i 2^i, n_i \in \{-1, 0, 1\}, n_0 = 1

5: for j \leftarrow l - 1 down do 0

6: f \leftarrow f^2 \cdot \frac{g_{V,V}(S)g_{2V}(Q')}{g_{2V}(S)g_{V,V}(Q')}

7: V \leftarrow 2V

8: if n_i = 1 then
                     if n_j = 1 then
  8:
                         f \leftarrow f \cdot \frac{g_{V,P}(S)g_{V+P}(Q')}{g_{V+P}(S)g_{V,P}(Q')}
V \leftarrow V + P
if n_j = -1 then
  9:
  10:
  11:
                                  f \leftarrow f \cdot f_{-1} \cdot \frac{g_{V,P}(S)g_{V-P}(Q')}{g_{V-P}(S)g_{V,P}(Q')} 
V \leftarrow V - P 
  12:
  13:
                         return f
  14:
  Signed
  Miller
  Al-
  go-
 ɔritこのように符号付きで展開する方法は後述のアルゴリズムでも同様に用いることができる.th
```

速化手法 su pringular curc おける Rd dTペアリングの高速化手法が B reらによっていくつか提案された?それを次に列挙する部分体の要素による乗算埋め込み次数 k の因子に