問5.2

[署名生成]

1. $m' \leftarrow H(m)$
2. generate random variable $r \in \mathbb{Z}_q^*$
3. $u \leftarrow (g^r \bmod p) \bmod q$
4. if $u=0$, then go to 3.
5. $u \leftarrow r^{-1}(m' + xu) \bmod q$.
6. if $u=0$, then go to 3
7. return $(u, u)$

[署名検証]

1. $m' \leftarrow H(m)$
2. $u' \leftarrow (g^{m'/u} y^{u/u} \bmod p) \bmod q$.
3. if $u \equiv u' \bmod q$
4. return OK
5. else
7. return NG

$p, q$は十分に大きいとする.

乗算回数：3

べき乗回数：3

逆元計算回数：2