問5.1

gの位数lは、$l=11$ ($\because \gcd(g,p)=1$ かつ、$g^{11} \bmod p = 1$ より)

$y = 2^2 \bmod 23 = 4$

$u_1 = 2^3 \bmod 23 = 8$

$u = 8 \bmod 11 = 8$

$r^{-1} = 4$

$u = r^{-1}(H(m) + xu) \bmod l = 4(4 + 2\cdot 8) \bmod 11 = 3$

∴署名は、$(u, u) = (8, 3)$

$u^{-1} = 4$

$u' = (2^{4\cdot 4} \cdot 4^{8\cdot 4} \bmod 23) \bmod 11 = 8$

$u \equiv u'$ であるから OK.