(G3)を示す.

$(b,y)=\left(-ax^{-2},x^{-1}\right)$とおけば,

$(a,x)\cdot(b,y)=(a,x)\cdot\left(-ax^{-2},x^{-1}\right)=(0,1)=e$,

$(b,y)\cdot(a,x)=\left(-ax^{-2},x^{-1}\right)\cdot(a,x)=(0,1)=e$.

よって, $(a,x)\cdot(b,y)=(b,y)\cdot(a,x)=e$.　　*Q.E.D.*

[4]

(1)

(ユークリッドの互除法使用)

$40=5\times7+5\cdots$①,

$7=1\times5+2\cdots$②,

$5=2\times2+1\cdots$③,

$2=2\times1$,

より,

$\gcd(e,L)=\gcd(7,40)=1$

$=5-2\times2$　　(③より)

$=5-2\times(7-1\times5)$　　(②より)

$=3\times5-2\times7$

$=3\times(40-5\times7)-2\times7$　　(①より)

$=-17\times7+3\times40=-17e+3L$.

よって, $(s,t)=(-17,3)$.

(2)

$$d=e^{-1}=7^{-1}=7^{\varphi(40)-1}=7^{15}=\left(7^2\right)^7\times7\equiv9^7\times7=\left(9^2\right)^3\times9\times7\equiv1\times9\times7=63\equiv23\pmod{40}.$$

($\because\ \varphi(40)=\varphi\left(2^3\times5\right)=\varphi\left(2^3\right)\times\varphi(5)=2^2(2-1)\times(5-1)=16$,

$7^2=49\equiv9\pmod{40}$, $9^2=81\equiv1\pmod{40}$.)

$\therefore d=23$.

(3)

まず, $de\equiv1\pmod{L}$であるので, ある整数kを用いて,

$de=kL+1$と書ける.

また,

$\varphi(n)=\varphi(pq)=\varphi(p)\times\varphi(q)=(p-1)(q-1)$.

(↑$\because\ p$, qは素数)

なので,

$$c^d=x^{de}=x^{kL+1}=x^{k(p-1)(q-1)+1}=x^{k\varphi(n)+1}=x\left(x^{\varphi(n)}\right)^k\equiv x\pmod{n}.$$

(↑$\because$オイラーの定理より, $x^{\varphi(n)}\equiv1\pmod{n}$)

$\therefore$送信メッセージが求まる.　　*Q.E.D.*