3

(1) $m = 3, 4, 5, 6, 7$ について、法 m に関する掛け算表を埋めてみよ。(m の値による様子の違いを観察せよ。)

$m = 3$

$\times$	1	2
1		
2		

$m = 4$

$\times$	1	2	3
1			
2			
3			

$m = 5$

$\times$	1	2	3	4
1				
2				
3				
4				

$m = 6$

$\times$	1	2	3	4	5
1					
2					
3					
4					
5					

$m = 7$

$\times$	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

(2) 法 $p = 7$ に関する演算において、

(a) $4x = 5$ となる x を表から探すと、唯一つ存在し、$x = \square$ である。
（この x のことを $5/4$ と定める。）

(b) $4z = 1$ となる z を表から探すと、唯一つ存在し、$z = \square$ である。
（この z のことを $1/4$ と定める。これは法 7 に関する 4 の “逆数” と考えられ、4^{-1} とも表わす。）

(c) 4 での割り算はその逆数 4^{-1} を掛けることでも計算できる。実際、

$$x = 5/4 = 5 \times 4^{-1} = 5 \times \square = \square$$

となり、上の結果と一致する。

(3) 法 $p = 7$ に関する演算を用いて秘密分散を行なった。配布した紙片に書いてある自分の鍵と他の誰かの人の鍵とから秘密情報 b を復元せよ。

$$y \equiv ax + b \pmod 7$$

- 自分の鍵 $(x_0, y_0) = (\quad , \quad)$
- もう一人の鍵 $(x_1, y_1) = (\quad , \quad)$
（違う値を持つ人に見せてもらうこと）
- 直線の傾き（ランダムに選ばれた秘密のパラメタ）

$$a = \frac{y_1 - y_0}{x_1 - x_0} = \frac{\square - \square}{\square - \square} = \frac{\square}{\square} = \square$$

- 秘密情報

$$b = y_0 - ax_0 = \square - \square \cdot \square = \boxed{\square}$$

(4) （次回予告）Caesar 暗号で暗号化された次の文字列を解読せよ。

phq dqg zrphq iru rwkhuv zlwk rwkhuv