

Q1

$$(\mathbb{Z}/153\mathbb{Z}^*, \cdot)$$

cars les nombres co-premiers avec 153.

$$\phi(153) = \phi(3^2 \cdot 17)$$

$$= 2 \cdot 3 \cdot 16$$

$$= 6 \cdot 16$$

$$= 36 + 60 = \underline{96}$$

$$9 \cdot 10 = 90$$

$$9 \cdot 7 = 63$$

$$(p-1) \cdot p^{k-1}$$

Q2

$$[t_1^{e_1}]_m = c_1$$

$$[t_2^{e_2}]_m = c_2$$

$$(c_1 \cdot c_2) [m]$$

$$\equiv [t_1^{e_1} \cdot t_2^{e_2}]_m$$

$$= [t_1^{e_1 d} \cdot t_2^{e_2 d}]_m$$

$$t_1^{(e_1 + e_2)d}$$

$$(e_1, e_2)^{e_1 e_2}$$

Q3

(a) $Z/10Z = \{1, 3, 7, 9\} \frac{1}{4}$
 $\{2, 4, 8, 10\} \frac{1}{4}$

S_2

	1	3	5	7	9	
S_1	1	3	5	7	9	
	1/4	0	0	0	0	= 1/4
	1/8	1/8	0	0	0	= 1/4
	1/16	1/16	1/16	1/16	0	= 1/4
	1/16	1/16	0	1/16	1/16	= 1/4

$$\begin{array}{c} \parallel \quad \parallel \quad \parallel \quad \parallel \quad \parallel \\ 1/2 \quad 1/4 \quad 1/16 \quad 1/8 \quad 1/16 \end{array}$$

$$Z = \{1, 2, 3, 4, 5, 6\}$$

$$Z / S Z^* = \{1, 2, 3, 4\}$$

$$Z / 2 Z^* = \{1\}$$

$$4 = \{1, 3\}$$

$$8 = \{1, 3, 5, 7\}$$

$$Z / 6 Z^* = \{1, 5\}$$

⑥ No because probabilities change

⑦

$$H(S_n / S_1 \dots S_{n-1}) \leq H(S_n)$$

Si on connaît S_{n-1} , on connaît le

groupe $\mathbb{Z}/(S_n + 1) \mathbb{Z}^*$, dans ce
groupe uniformément distribué

4 6 8 10

$H(S_n / S_{n-1})$

$S_n = 1$
 \Rightarrow la proba qu'il soit 1
 avant $+ \frac{1}{2}$ si c 3, etc.

$$\text{si } S_{n-1} = 3 : \frac{1}{8} \text{ "x2"}$$

$$= 7 : \frac{1}{16} \text{ "x4"}$$

$$= 9 : \frac{1}{16} \text{ "x4"}$$

$$= 5 : \frac{1}{16} \text{ "x4"}$$

$$= 1, \frac{1}{4} \text{ "x1"}$$

$$p_{Sn}(3) = p_{Sn-1}(5) \cdot \frac{1}{4}$$

$$+ p_{Sn-1}(3) \cdot \frac{1}{2}$$

$$+ p_{Sn-1}(7) \cdot \frac{1}{4}$$

Question 4

(a) for (e, d) to be valid exp,

$$ed + k\phi(m) = 1 \Rightarrow \text{impossible}$$

$$\phi(pq) = (p-1)(q-1) = 52 \cdot 6 \cdot 10$$

$$\begin{array}{l} 123 \cdot 20 \\ = 2460 \Delta 660 \end{array} \left| \begin{array}{l} 123 \cdot 5 = 615 \\ 123 \cdot 5 = 615 \end{array} \right| \begin{array}{l} = 312 \cdot 10 \\ = 3120 \end{array}$$

$GCD(3120, 123)$	$a = bq + r$	q	u	v
$(3120, 123)$	$3120 = 123 \cdot 25 + 45$	25		
$(123, 45)$	$123 = 45 \cdot 2 + 33$	2		
$(45, 33)$	$45 = 33 \cdot 1 + 12$	1		
$(33, 12)$	$33 = 12 \cdot 2 + 9$	2		

(12, 9)

(9, 3)

$$12 = 9 \cdot 1 + 3$$

$$9 = 3 \cdot 3 + 0$$

1

⑥

e et d don't the more

$$\begin{array}{r} 12 \\ 223 \\ \cdot \quad 7 \\ \hline 1561 \end{array}$$

$$\begin{array}{r} 1 \\ 83 \\ \cdot \quad 61 \\ \hline 53 \\ 3180 \\ \hline \end{array}$$

Q5

8.10

$$\phi(15) = 2 \cdot 4 = 8$$

$$8278^{8k+1} = 8278 [15]$$

$$\begin{array}{r} 1500 \\ - \quad 3 \\ \hline 1497 \end{array}$$

$$7500$$

$$28$$

$$= 15 \cdot 1 + 13$$

$$\begin{array}{r} 1500 \\ - \quad 2 \\ \hline 1498 \end{array}$$

$$\begin{array}{r} 778 \quad 150 \\ - \quad 5 \\ \hline 773 \end{array}$$

		mod 5				
		0	1	2	3	4
mod 3	0	0	6	12	3	9
	1	10	1	7	(13)	4
	2	5	11	2	8	14

$$ed + \textcircled{k} \phi(m) = 1$$

↓

$$k \text{ cm}(p-1, q-1)$$

$$\Rightarrow [ed]_k = 1$$

$$\Rightarrow 319 \cdot 23 \equiv \textcircled{x} [780]$$

$$\begin{array}{r}
 1 \\
 349 \\
 - 23 \\
 \hline
 1957 \\
 + 6380 \\
 \hline
 7337
 \end{array}$$

$$780 - 9$$

$$\begin{array}{r}
 7 \\
 780 \\
 - 9 \\
 \hline
 00
 \end{array}$$