HW 2

Thursday, February 6, 2020 10:47

Problem #1: Find the distribution for permutations over P_7.

Distribution of all permutations over P_7.

\# of permutations = $7! = 5040$

7	6	5	4	3	2	1

count $= \frac{7\times 6}{2!} \times \frac{5\times4\times3\times2\times1}{5!} = 21$

(i.e. 1,1,1,1,1,1,1)

Structure	Count	order	
e (identity)	1	1	LCM(1,1,...1) = 1
2,1,1,1,1,1	$\frac{7\times6}{2} = 21$	2	LCM(2,1,1,1,...) = 2
3,1,1,1,1	$\frac{7\times6\times5}{3} = 70$	3	LCM(3,1,1,1,1) = 3
4,1,1,1	$\frac{7\times6\times5\times4}{4} = 210$	4	LCM(4,1,1,1) = 4
5,1,1	$\frac{7\times6\times5\times4\times3}{5} = 504$	5	LCM(5,1,1) = 5
6,1	$\frac{7\times6\times5\times4\times3\times2}{6} = 840$	6	LCM(6,1) = 6
3,2,1,1	$\frac{7\times6\times5}{3}\cdot\frac{4\times3}{2} = 420$	6	LCM(3,2,1,1) = 6
3,3,1	$\frac{7\times6\times5}{3}\times\frac{4\times3\times2}{3}\cdot\frac{1}{2!} = 280$	3	LCM(3,3,1) = 3
2,2,2,1	$\frac{7\times6}{2}\times\frac{5\times4}{2}\times\frac{3\times2}{2}\cdot\frac{1}{3!} = 105$	2	LCM(2,2,2,1) = 2
4,2,1	$\frac{7\times6\times5\times4}{4}\times\frac{3\times2}{2} = 630$	4	LCM(4,2,1) = 4
4,3	$\frac{7\times6\times5\times4}{4}\times\frac{3\times2\times1}{3} = 420$	12	LCM(4,3) = 12
3,2,2	$\frac{7\times6\times5}{3}\times\frac{4\times3}{2}\times\frac{2\times1}{2}\times\frac{1}{2!} = 210$	6	LCM(3,2,2) = 6
5,2	$\frac{7\times6\times5\times4\times3}{5}\times\frac{2\times1}{2} = 504$	10	LCM(5,2) = 10
2,2,1,1,1	$\frac{7\times6}{2}\times\frac{5\times4}{2}\cdot\frac{1}{2!} = 105$	2	LCM(2,2,1,1,1) = 2
7	$\frac{7\times6\times5\times4\times3\times2\times1}{7} = 720$	420	LCM(7,6,5,4,3,2,1) = 420
	count = 5040		

Class Problem #2: How many involutory substitution keys are in the English language?

Involutory keys are of order 2

Involutory keys	Count $= \dfrac{26!/(26-2n)!}{2^n \cdot n!}$

Involutory Keys	$\text{Count} = \frac{26!/(26-2n)!}{2^n \cdot n!}$
$n=1$ 2,1,1,...,1	$\frac{26\times25}{2} = \frac{26!/24!}{2^1\cdot1!} = 325$
$n=2$ 2,2,1,1,...,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{1}{2!} = \frac{26!/22!}{2^2\cdot2!} = 44,850$
$n=3$ 2,2,2,1,1,...,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{1}{3!} = \frac{26!/20!}{2^3\cdot3!}$ 3,453,450
2,2,2,2,1,1,...,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{20\times19}{2}\times\frac{1}{4!} = 164,038,875$
2,2,2,2,2,1,1,...,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{20\times19}{2}\times\frac{18\times17}{2}\times\frac{1}{5!} = 5,01958958\cdot10^9$
2,2,2,2,2,2,1,1,...,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{20\times19}{2}\times\frac{18\times17}{2}\times\frac{16\times15}{2}\times\frac{1}{6!} =$ 100,391,791,500
2,2,...,2 (×7) 1,1,...,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{20\times19}{2}\times\frac{18\times17}{2}\times\frac{16\times15}{2}\times\frac{14\times13}{2}\times\frac{1}{7!} =$ 1,305,093,289,500
2,2,...,2 (×8) 1,1,...,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{20\times19}{2}\times\frac{18\times17}{2}\times\frac{16\times15}{2}\times\frac{14\times13}{2}\times\frac{12\times11}{2}\times\frac{1}{8!} =$ 10,767,019,638,375
2,2,...,2 (×9) 1,1,...,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{20\times19}{2}\times\frac{18\times17}{2}\times\frac{16\times15}{2}\times\frac{14\times13}{2}\times\frac{12\times11}{2}\times\frac{10\times9}{2}\times\frac{1}{9!} =$ 53,835,098,191,875
2,2,...,2 (×10) 1,1,...,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{20\times19}{2}\times\frac{18\times17}{2}\times\frac{16\times15}{2}\times\frac{14\times13}{2}\times\frac{12\times11}{2}\times\frac{10\times9}{2}\times\frac{8\times7}{2}\times\frac{1}{10!} =$ 150,738,274,937,250
2,2,2,...,2 (×11) 1,1,1,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{20\times19}{2}\times\frac{18\times17}{2}\times\frac{16\times15}{2}\times\frac{14\times13}{2}\times\frac{12\times11}{2}\times\frac{10\times9}{2}\times\frac{8\times7}{2}\times\frac{6\times5}{2}\times\frac{1}{11!} =$ 205,552,193,096,250
2,2,...,2 (×12) 1,1	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{20\times19}{2}\times\frac{18\times17}{2}\times\frac{16\times15}{2}\times\frac{14\times13}{2}\times\frac{12\times11}{2}\times\frac{10\times9}{2}\times\frac{8\times7}{2}\times\frac{6\times5}{2}\times\frac{4\times3}{2}\times\frac{1}{12!} =$ 102,776,096,548,125
2,2,...,2 (×13)	$\frac{26\times25}{2}\times\frac{24\times23}{2}\times\frac{22\times21}{2}\times\frac{20\times19}{2}\times\frac{18\times17}{2}\times\frac{16\times15}{2}\times\frac{14\times13}{2}\times\frac{12\times11}{2}\times\frac{10\times9}{2}\times\frac{8\times7}{2}\times\frac{6\times5}{2}\times\frac{4\times3}{2}\times\frac{2\times1}{2}\times\frac{1}{13!} =$ 7,905,853,580,625

Therefore, adding all counts of involutory keys together, Therefore, adding all counts of involutory keys together, the total number of keys is:

532,985,208,200,575 or 5.32 * 10^14 total number of keys

1.11 (a) Suppose that $K = (a, b)$ is a key in an *Affine Cipher* over $\mathbb{Z}_n$. Prove that K is an involutory key if and only if $a^{-1} \bmod n = a$ and $b(a+1) \equiv 0 \pmod{n}$.

(b) Determine all the involutory keys in the *Affine Cipher* over $\mathbb{Z}_{15}$.

(c) Suppose that $n = pq$, where p and q are distinct odd primes. Prove that the number of involutory keys in the *Affine Cipher* over $\mathbb{Z}_n$ is $n + p + q + 1$.

a.) $K = (a, b)$ is involutory key iff $a(ax+b)+b \equiv x \bmod n$ for all x in $\mathbb{Z}_n$

By simply algebraically manipulating the variables:

$a(ax+b)+b = a^2x + ab + b^2 \equiv a^2x + b(a+1) \pmod{n}$

In order for the RHS to be true,

$a^2x + b(a+1) \pmod{n}$ must be able to become $x \pmod{n}$.

This means that $a^2 \equiv 1$ and $b(a+1) \equiv 0$

so that $((1)x + (0)) \pmod{n} \equiv x \pmod{n}$ ✓

b.) All involutory keys in Affine Cipher over $\mathbb{Z}_{15}$.

A key a is an involutory key in an Affine Cipher

iff $a^2 \equiv 1 \pmod{n}$, $\Rightarrow a^2 \equiv 1 \pmod{15}$ in $\mathbb{Z}_{15}$,

so $a^2 \equiv 1 \pmod{15}$

and $b \equiv -a^{-1}b \pmod{15}$, or $b + ab \equiv 0 \pmod{15}$

$\Downarrow$

$b(1+a) \equiv 0 \pmod{15}$

By trial & error

if $a = 0$ $\quad 0^2 \not\equiv 1 \pmod{15}$

if $a = 1$ $\quad (1)^2 \equiv 1 \pmod{15}$ ✓

$\Rightarrow$ for $b(1+1) \equiv 0 \ \% \ 15$, to be true

$b = 0$.

So $a = 1, b = 0$ is a key

a	b	$a^2 \equiv 1\%15$	b such that b(1+a)≡0%15	Valid?	
0		X	X	No	
1	0	✓	✓	Yes	
2		X	X	No	
3		X	X	No	
4	0, 3, 6, 9, 12	✓	✓	Yes	
5		X	X	No	
6		X	X	No	
7		X	X	No	
8		X	X	No	
9		X	X	No	
10		X	X	No	
11	0, 5, 10	✓	✓	Yes	
12		X	X	No	
13		X	X	No	
14	(Any key) 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	✓	✓	Yes	

Thus involutory keys are:

$a = 1, b = 0$

$a = 4, b = 0, 3, 6, 9, 12$

$a = 11, b = 0, 5, 10$

$a = 14, b = x \in Z_{15}$ $(0, 1, 2, \ldots 14)$

C.) Possible values for involutory keys for a.

1 value → 1.) $a \equiv 1 \ \% \ p$ ($b = 0$ since $b(1+1) \equiv 0 \ \% \ p$ has $b = 0$)

\+

n values → 2.) $a \equiv -1 \ \% \ q$ ($b = n$ since $b(1-1) \equiv 0 \ \% \ p$ can be any value in n)

\+

p values → 3.) a where $a \equiv 1 \ \% \ p$ and $a \equiv -1 \ \% \ q$ ($b \equiv 0 \ \% \ q$, so there are p possible values)

\+

q values → 4.) a where $a \equiv -1 \ \% \ p$ & $a \equiv 1 \ \% \ q$ ($b \equiv 0 \ \% \ p$, so there are q possible values of b)

→ Thus, the total number of values for b is $1 + n + p + q$.

1.16 (a) Suppose that π is the following permutation of $\{1, \ldots, 8\}$:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

Compute the permutation π^{-1}.

(b) Decrypt the following ciphertext, for a *Permutation Cipher* with $m = 8$, which was encrypted using the key π:

TGEEMNEL|NNTDROEO|AAHDOETC|SHAEIRLM.

a.) $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 1 & 8 & 3 & 5 & 7 \end{pmatrix}$

Testing π^{-1}:

$$\pi \circ \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 6 & 2 & 7 & 3 & 8 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 1 & 8 & 3 & 5 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = e$$

$\therefore$ π^{-1} is correct since $\pi \circ \pi^{-1} = e$

b.) With $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 6 & 2 & 7 & 3 & 8 & 5 \end{pmatrix}$ $(m=8)$

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM

ETNGEEA DNONETOR DAEATHCO ESRHLAMI

which doesn't translate to any sensible plaintext.

BUT, using $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 1 & 8 & 3 & 5 & 7 \end{pmatrix}$

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM

GENTLEME NDONOTRE ADEACHOT HERSMAIL,

which translates to

Gentlemen do not read each other's mail

when decrypted using π^{-1} as the key.

1.17 (a) Prove that a permutation π in the *Permutation Cipher* is an involutory key if and only if $\pi(i) = j$ implies $\pi(j) = i$, for all $i, j \in \{1, \ldots, m\}$.

(b) Determine the number of involutory keys in the *Permutation Cipher* for $m = 2, 3, 4, 5$ and 6.

a.) A permutation π is involutory key iff

$\pi(\pi(i)) = i$ for every i.

With $\pi(i) = j$, it must also be true ~~that~~ $\pi(j) = i$

j replaces $\pi(i)$ in $\pi(\pi(i))$

b.) An involutory key of a permutation cipher must consist of fixed points & cycles of length two.

$m=2$: Cycles of $(1,1)$ and (2) are valid.

count of 1 count of 1

So there are $\underline{2}$ involutory permutations for $m=2$

$m=3$: Cycles of $(1,1,1)$, $(2,1)$

$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

1 $\qquad \frac{3 \cdot 2}{2} \cdot \frac{1}{1!} = 3$

$1 + 3 = 4$

So there are 4 involutory keys for $m=3$

$m=4$: Cycles of $(1,1,1,1)$, $(2,1,1)$, and $(2,2)$ possible.

1 $\qquad \frac{4 \cdot 3}{2} \cdot \frac{2 \cdot 1}{2} = 6$ $\qquad \frac{4 \cdot 3}{2} \cdot \frac{2 \cdot 1}{2} \cdot \frac{1}{2} = 3$

$1 + 6 + 3 = 10$

So, there are 10 involutory keys for $m=4$

$m=5$: Cycles of $(1,1,1,1,1)$, $(2,1,1,1)$, $(2,2,1)$

1 $\qquad 5 \times 4$

$$1 \qquad \frac{5\times4}{2}\cdot\frac{3\cdot2\cdot1}{3!}=10 \qquad \frac{5\times4}{2}\times\frac{3\times2}{2}\cdot\frac{1}{2!}=15$$

$1+10+15=26$

So, there are 26 involutory keys for $m=5$

$m=6$: cycles of $(1,1,1,1,1,1)$, $(2,1,1,1,1)$, $(2,2,1,1)$, $(2,2,2)$

$$1 \qquad \frac{6\times5}{2}=15 \qquad \frac{6\times5}{2}\times\frac{4\times3}{2}\times\frac{1}{2!}=45$$

$$\frac{6\times5}{2}\times\frac{4\times3}{2}\times\frac{2\times1}{2}\times\frac{1}{3!}=15$$

$1+15+45+15=76$

Thus, the total number of involutory keys is 76.

In summary,

$m=2$: 2 involutory permutations

$m=3$: 4 " "

$m=4$: 10 " "

$m=5$: 26 " "

$m=6$: 76 " "