Problem 1.

$H(N_1, N_2) = Enc(IK, Enc(IK, N_1) \oplus N_2)$

Let $N_2 = Enc(IK, N_1) \oplus Enc(IK, M_1) \oplus M_2$.

$= Enc(IK, Enc(IK, N_1) \oplus Enc(IK, N_1) \oplus Enc(IK, M_1) \oplus M_2$

$= Enc(IK, Enc(IK, M_1) \oplus M_2)$

$= H(M_1, M_2) = h$

Thus, we choose $N_2 = Enc(IK, N_1) \oplus Enc(IK, M_1) \oplus M_2$, which can make $H(M_1 M_2) = H(N_1 N_2) = h$.

So, H does not satisfy the property of second image resistance. □

Problem 2.

$f = 0$

$\Rightarrow \sin 2\pi (0) x = \sin 0 = 0$

$\Rightarrow \sum_{i=0}^{7} \vec{a_i} \cdot \sin 0 = 0$ #

$f = 1$

$\Rightarrow \sin 2\pi \, 1/8 \, x = \sin \pi/4 \, x$

$\Rightarrow \sum_{i=0}^{7} \vec{a_i} \cdot \sin \pi/4 \, i$

$= 0 \cdot \sin \pi/4 \cdot 0 + 1 \cdot \sin \pi/4 \cdot 1 + 0 \cdot \sin \pi/4 \cdot 2 + 3 \cdot \sin \pi/4 \cdot 3 +$
$0 \cdot \sin \pi/4 \cdot 4 + 1 \cdot \sin \pi/4 \cdot 5 + 0 \cdot \sin \pi/4 \cdot 6 + 3 \sin \pi/4 \cdot 7$

$= 0 + 1/\sqrt{2} + 0 + 3/\sqrt{2} + 0 + (-1/\sqrt{2}) + 0 + (-3/\sqrt{2}) = 0$ #

$f = 2$

$\Rightarrow \sin 2\pi \, 2/8 \, x = \sin \pi/2 \, x$

$\Rightarrow \sum_{i=0}^{7} \vec{a_i} \sin \pi/2 \, x$

$= 0 \cdot \sin \pi/2 \cdot 0 + 1 \cdot \sin \pi/2 \cdot 1 + 0 \cdot \sin \pi/2 \cdot 2 + 3 \cdot \sin \pi/2 \cdot 3 +$
$0 \cdot \sin \pi/2 \cdot 4 + 1 \cdot \sin \pi/2 \cdot 5 + 0 \cdot \sin \pi/2 \cdot 6 + 3 \cdot \sin \pi/2 \cdot 7$

$= 0 + 1 + 0 + (-3) + 0 + 1 + 0 + (-3) = -4$ #

$f = 3$

$\Rightarrow \sin 2\pi \, 3/8 \, x = \sin 3/4 \pi x$

$\Rightarrow \sum_{i=0}^{7} \vec{a_i} \sin 3/4 \pi x$

$= 0 \cdot \sin 3/4 \pi \cdot 0 + 1 \cdot \sin 3/4 \pi \cdot 1 + 0 \cdot \sin 3/4 \pi \cdot 2 + 3 \cdot \sin 3/4 \pi \cdot 3 +$
$0 \cdot \sin 3/4 \pi \cdot 4 + 1 \cdot \sin 3/4 \pi \cdot 5 + 0 \cdot \sin 3/4 \pi \cdot 6 + 3 \cdot \sin 3/4 \pi \cdot 7$

$= 0 + 1/\sqrt{2} + 0 + 3/\sqrt{2} + 0 + (-1/\sqrt{2}) + 0 + (-3/\sqrt{2}) = 0$ #

Problem 3.

$$e = 2.71828\cdots$$

$$\to 2+0.71828\cdots = 2+\cfrac{1}{\cfrac{1}{0.71828\cdots}} = 2+\cfrac{1}{1+0.39221\cdots}$$

$$= 2+\cfrac{1}{1+\cfrac{1}{\cfrac{1}{0.39221\cdots}}} = 2+\cfrac{1}{1+\cfrac{1}{2+0.54964\cdots}}$$

$$= 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{\cfrac{1}{0.54964\cdots}}}} = 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1.819350\cdots}}}$$

$$= 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{\cfrac{1}{0.819350\cdots}}}}} = 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1.220479\cdots}}}}$$

$$= 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{\cfrac{1}{0.220479\cdots}}}}}} = 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4.53557\cdots}}}}}$$

$$= 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{\cfrac{1}{0.53557\cdots}}}}}}} = 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1.86715\cdots}}}}}}$$

$$= 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{\cfrac{1}{0.86715\cdots}}}}}}}} = 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1.15319\cdots}}}}}}}$$

$$\Rightarrow 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1}}}}}}}$$

$$\Rightarrow \left(4+\frac{1}{2}\right)^{-1} = \frac{2}{9}$$

$$\left(\frac{2}{9}+1\right)^{-1} = \frac{9}{11}$$

$$\left(\frac{9}{11}+1\right)^{-1} = \frac{11}{20}$$

$$\left(\frac{11}{20}+2\right)^{-1} = \frac{20}{51}$$

$$\left(\frac{20}{51}+1\right)^{-1} = \frac{51}{71}$$

$$2+\frac{51}{71} = \frac{193}{71} = 2.718309\cdots$$

$$e = 2.7182818\cdots$$

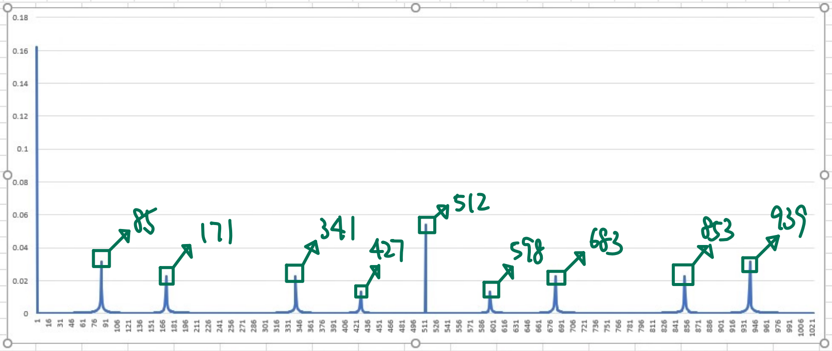
$$\Rightarrow \frac{193}{71} \quad \#$$

Problem 4

$M=39$, $a=7$, sample $N=1024$ points, $g(x)=a^x \bmod M$

(a) At first we compute $g(x_i)=7^{x_i} \bmod 39$, for $x_i=0,1,2,3,\cdots,1023$.
The we have $[1,7,10,31,22,37,25,19,16,34,4,28,1,7,\cdots,31]$
Then put this sequence into DFT.
And transform the result of DFT by IMABS into the numbers which are larger than zero.

With these numbers, taking summation on them.
Then divide these numbers by the summation to calculate the proportion, and get this diagram.



Take $d_1=85$, $d_2=171$, $d_3=341$

$$\frac{d_1}{1024}=\frac{85}{1024}\simeq\frac{1}{12}$$

$$\left|\frac{1}{12}-\frac{85}{1024}\right|=0.000325\cdots\leq\frac{1}{2N}\Rightarrow 12 \text{ is a candidate}$$

$\hookrightarrow$ < 5-bit long

$$\frac{d_2}{1024}=\frac{171}{1024}\simeq\frac{1}{6}$$

$$\left|\frac{1}{6}-\frac{171}{1024}\right|=0.000325\cdots\leq\frac{1}{2N}\Rightarrow 6 \text{ is also a candidate}$$

$\hookrightarrow$ < 5-bit long

$$\frac{d_3}{1024}=\frac{341}{1024}\simeq\frac{1}{3}$$

$$\left|\frac{1}{3}-\frac{341}{1024}\right|=0.000325\cdots\leq\frac{1}{2N}\Rightarrow 3 \text{ is a candidate, too}$$

Take $s = 12 \Rightarrow 7^{12} \bmod 39 = 1$

$s/2 = 6 \Rightarrow 7^{6} \bmod 39 = 25$

$25 \pm 1 = 24, 26$

$\left.\begin{array}{l} \gcd(24, 39) = 3 \\ \gcd(26, 39) = 13 \end{array}\right\} 3 \times 13 = 39$

We successfully factor $M = 39$ as two factors 3 and 39. #

(b) point 0 = 0.162137096

point 85 = 0.031347013

point 171 = 0.022485928

point 341 = 0.022425283

point 427 = 0.013277914

point 512 = 0.054132436

point 597 = 0.013277914

point 683 = 0.022425283

point 853 = 0.022485928

point 939 = 0.031347013 $\Rightarrow$ sum = 0.395341808 #