

2 First, in the CSV file, we consider $(x_i; y_i) \pmod{6}$
 let $A(u, v) = \{(x, y) \in \text{CSV} \mid x \equiv u \pmod{6} \text{ and } y \equiv v \pmod{6}\}$
 We will run a Python script to find $|A(u, v)|$ for $0 \leq u, v < 6$.
 The script will be attached later. We obtain the following table for $|A(u, v)|$:

$v \backslash u$	0	1	2	3	4	5
0	8	9	11	2	16	8
1	7	22	7	3	6	9
2	25	5	8	5	7	4
3	9	18	5	10	4	7
4	10	7	9	2	20	6
5	7	7	4	24	9	4

We try to choose a small set S that contains all 90 v .
 Note that if we choose $(x; y) \in A(u, v)$, then we will choose $(x'; y') \in A(u, v')$ for $v' \neq v$. Therefore, for each $u \in \{0, 1, \dots, 5\}$, we choose exactly one v , and let S contain all elements in $A(u, v)$.

Now we just need to choose v for each u . We will try the easiest way. For each u , we choose v such that $|A(u, v)|$ is maximal. For example, when $u = 0$, we choose $v = 4$, when $u = 1$, we choose $v = 1$.

let $\text{mod6list} = \{(0; 4); (1; 1); (2; 0); (3; 1); (4; 4)$

then for each u , mod6list contain (u, v) such that $|A(u, v)|$ is maximal.

Our set S will be: $S = \{(x, y) \in \text{CSV} \mid (x, y) \in \text{mod6list} \pmod{6}\}$

Note that $\forall (x, y)$ and $(x', y') \in S$ we have:

$$2 \mid x' - x \Rightarrow 2 \mid y' - y \text{ and } 3 \mid x' - x \Rightarrow 3 \mid y' - y$$

This increases the chance of S containing all the 90 correct values.

The script that print all elements in S will be attached later. Now, we have $|S| = 125$ and we need to

choose 2 monic polynomials $A(x)$ and $B(x)$ such that $y_i = \frac{A(x_i)}{B(x_i)}$ for at least 90 indices of

i in S in \mathbb{Z}_{2022} . I will use A, B instead of f, g .

Consider $A(x), B(x)$ in $\mathbb{Z}_{337}[x]$. We will use something similar to Berlekamp-Welch algorithm to restore A and B in $\mathbb{Z}_{337}[x]$

To do so, let's find 2 polynomials A' and B' of degree 51 and monic such that $y_i = \frac{A'(x_i)}{B'(x_i)}$ \forall

$(x_i, y_i) \in S$ in \mathbb{Z}_{337} .

$$\text{let } P(x) = \prod_{\substack{(u,v) \in S \\ v \neq \frac{A(u)}{B(u)}}} (x - u) \cdot A(x)$$

$$Q(x) = \prod_{\substack{(u,v) \in S \\ v \neq \frac{A(u)}{B(u)}}} (x - u) \cdot B(x)$$

VKA

Note that $\frac{P(x)}{Q(x)} = \frac{A(x)}{B(x)}$ and $y_i Q(x_i) = P(x_i) \forall (x_i, y_i) \in S$ in \mathbb{Z}_{337} .

We will claim that: If there exists such A, B , then

$$\frac{A'(x)}{B'(x)} = \frac{P(x)}{Q(x)} \text{ in } \mathbb{Z}_{337}[x]$$

Proof of claim:

First, note that $\# \{(u, v) \in S \mid v \neq \frac{A(u)}{B(u)} \text{ in } \mathbb{Z}_{337}\}$ thus $\deg P$ and $\deg Q \leq 51$.

Suppose $\frac{A'(x_i)}{B'(x_i)} = \frac{P(x_i)}{Q(x_i)} = y_i \forall (x_i, y_i) \in S$. Then

$$A'(x_i)Q(x_i) - B'(x_i)P(x_i) = 0 \text{ in } \mathbb{Z}_{337} \forall (x_i, y_i) \in S$$

However, the degree of $A'(x)Q(x) - B'(x)P(x)$ is at most 102, thus by Lagrange's theorem, $A'(x)Q(x) - B'(x)P(x) = 0$ in $\mathbb{Z}_{337}[x]$. In the other hand, we can choose $A' = P(x)$ and $B' = Q(x)$, then it is always possible to find $A'(x)$ and $B'(x)$. Thus we proved our claim.

Now, to find $A'(x)$ and $B'(x)$, note that for each $(x_i, y_i) \in S$ give us an equation $y_i = \frac{A'(x_i)}{B'(x_i)}$. Since there are 125 equations and 102 variables (the coefficients of A' and B'), we can easily find A' and $B'(x)$ by solving a system of equations.

The script for finding $A'(x)$ and $B'(x)$ will be attached.

VKA

After finding $A'(x)$ and $B'(x)$, we will factor them and find $A(x)$ and $B(x)$ in $\mathbb{Z}_{337}[x]$

The result is :

$$A(x) = x^{16} + 30x^{15} + 262x^{14} + 35x^{13} + 186x^{12} + 218x^{11} + 129x^{10} + 229x^9 + 184x^8 + 336x^7 + 70x^6 + 145x^5 + 182x^4 + 79x^3 + 146x^2 +$$

$$B(x) = x^{16} + 272x^{15} + 36x^{14} + 76x^{13} + 57x^{12} + 296x^{11} + 316x^{10} + 165x^9 + 42x^8 + 178x^7 + 125x^6 + 140x^5 + 239x^4 + 87x^3 + 104x^2 +$$

This is the result of $A(x)$ and $B(x)$ in $\mathbb{Z}_{337}[x]$ to find $A(x)$ and $B(x)$ in $\mathbb{Z}_{2022}[x]$, we need to find $A(x)$ and $B(x)$ in $\mathbb{Z}_2[x]$ and $\mathbb{Z}_3[x]$

In $\mathbb{Z}_2[x]$, we can choose $B(x) = x^{15}(x+1) + 1$, and in $\mathbb{Z}_3[x]$, we can choose $B(x) = x^{14}(x^2 - 1) + 1$

In $\mathbb{Z}_2[x]$, we can choose $A(x) = x^{15}(x+1) + x$ and in $\mathbb{Z}_3[x]$, we can choose $A(x) = x^{14}(x^2 - 1) + x^2 + x + 1$

The reason we choose A and B like that in $\mathbb{Z}_2[x]$ or $\mathbb{Z}_3[x]$ is because of considering $(\text{mod } 6)$ in the list mod6list and all $(x, y) \in S$ are in $\text{mod6list} (\text{mod } 6)$.

We have chosen $A(x)$ and $B(x)$ in $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ and now we just use CRT to find $A(x)$ and $B(x)$ in $\mathbb{Z}_{2022}[x]$. The script for finding $A(x)$ and $B(x)$ will be attached.

VKA

The final result of $A(x)$ and $B(x)$ in $\mathbb{Z}_{2022}[x]$ is:

$$A(x) = x^{16} + 1041x^{15} + 1610x^{14} + 372x^{13} + 186x^{12} + 1566x^{11} + 1140x^{10} + 1734x^9 + 1914x^8 + 858x^7 + 336x^6 + 1x^9 + 744x^5 + 1830x^4 + 1530x^3 + 1090x^2 + 1157x + 1912$$

$$B(x) = x^{16} + 609x^{15} + 710x^{14} + 750x^{13} + 1068x^{12} + 9x^9 + 1644x^{11} + 990x^{10} + 456x^9 + 1176x^8 + 42x^7 + 852x^6 + 462x^5 + 1488x^4 + 576x^3 + 1098x^2 + 1452x + 679.$$

The polynomial $A(x)$ and $B(x)$ satisfy:

$$y = \frac{A(x)}{B(x)} \text{ for at least 90 values of } (x, y) \text{ in CSV file.}$$

We conclude that we can choose:

$$f(x) = A(x) \text{ and } g(x) = B(x) \text{ in } \mathbb{Z}_{2022}[x]$$

Note: the script for finding $|A(u, v)|$ and all elements of S will be in `process_data_mod_6.py`

the script for finding $A(x)$ and $B(x)$ in $\mathbb{Z}_{337}[x]$ will be in `find_A(x) and B(x) in $\mathbb{Z}_{337}[x]$. so, similarly for finding $A(x)$ and $B(x)$ in $\mathbb{Z}_{2022}[x]$`