金融科技導論 HW3

許博翔 B10902085

December 12, 2023

$d = 2085$.

I used python to calculate the results and verify the signature. All problems are calculated using the same python code: `hw3.py`.

Problem 1.

x =10338857399563508035974916425421659830878883530402360147780309523428649499368 3

y =37057141145242123013015316630864329550140216928701153669873286428255828810018

Problem 2.

x =21505829891763648114329055987619236494102133314575206970830385799158076338148

y =98003708678762621233683240503080860129026887322874138805529884920309963580118

Problem 3.

x =53595164930737482131084084632769514911496653020800424158267026368137185428713

y =63502312947416917161968005114302548812120648010642713359130610753551326004793

Problem 4. $2085 = (100000100101)_2$.

Number of doubles: 11.

Number of additions: 3.

Problem 5. The number of additions can't be less than 3 in this case; therefore the fastest way to do it is the same as the original double and add algorithm.

Problem 6.

r =35042880449001488894090033250663472399319784323320325883456585786523239743048

s =86342853910302688101666388192984024312235233400696676159790806309913218704437

Problem 7. The result is true. (see the code)

Problem 8. Suppose that $p(x) = ax^2 + bx + c$.

One can see that $\begin{pmatrix} 1^2 & 1 & 1 \\ 2^2 & 2 & 1 \\ 3^2 & 3 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \\ 2085 \end{pmatrix}$.

$$\Rightarrow \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1^2 & 1 & 1 \\ 2^2 & 2 & 1 \\ 3^2 & 3 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 10 \\ 20 \\ 2085 \end{pmatrix} = \begin{pmatrix} 1027.5 \\ -3072.5 \\ 2055 \end{pmatrix} \equiv \begin{pmatrix} 6031 \\ 1931 \\ 2055 \end{pmatrix} \pmod{10007}.$$

$\therefore p(x) = 6031x^2 + 1931x + 2055.$