Projects 1
Part 1 (Chapter 1 Frequency Analysis):

For Project 1, you are required to write a detailed report explaining how you decrypted the provided ciphertext below, which was encrypted using a **substitution cipher**. Begin by describing the concept of substitution ciphers and their vulnerability to frequency analysis. In your favorite programming language, either **Python or C++**, write a program to calculate the relative frequency of all letters A–Z in the ciphertext. Compare these frequencies with the general English language letter frequencies provided in Table 1.1, focusing on substituting letters with closely matching frequency values. Since the ciphertext is relatively short, note that its letter frequencies may not perfectly align with standard English frequencies, so iterative refinement will be necessary. Document your approach, the challenges you encountered, and how you adjusted substitutions to make the decrypted text coherent.

Include screenshots of your program, the intermediate results, and the final output in the report. Additionally, provide the link to your executable code on an online platform, such as Google Colab (https://colab.research.google.com), where reviewers can run your code and verify the results. Report of your work should be exported into a PDF file, ensuring it contains the detailed explanation of each step, the screenshots, and the online code link. Submit the final PDF file on Brightspace. Your report should be clear, thorough, and demonstrate both the logic behind your approach and the practical implementation of your solution. The ciphertext is given below:

```
    lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi
     bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx
 ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
  yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk
             lmird jk xjubt trmui jx ibndt

   wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi
 iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m
 vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr
  jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii
ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh
 mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb
    bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd
 wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr
      riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb
```

Table 1.1 Relative letter frequencies of the English language

Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0906
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007

Part 2 (Practicing Modular Arithmetics Calculation without Calculator):
Please Show your work step by step

Problem 1: Compute the result without a calculator.

(A) $15 \cdot 29 \bmod 13$

(B) $2 \cdot 29 \bmod 13$

(C) $2 \cdot (-3) \bmod 13$

(D) $(-11) \cdot 3 \bmod 13$

Problem 2: Compute without a calculator:

(A) $1/5 \bmod 13$

(B) $1/5 \bmod 7$

(C) $3 \cdot 2/5 \bmod 7$

Problem 3: For each of the following find an integer x that satisfies the equation:

(A) $5x = 4 \bmod 3$

(B) $7x = 6 \bmod 5$

(C) $9x = 8 \bmod 7$

Problem 4: Compute x as far as possible without a calculator. Where appropriate, make use of a smart decomposition of the exponent as shown in the example in Sect. 1.4.1:

(A) $x = 3^2 \bmod 13$

(B) $x = 7^2 \bmod 13$

(C) $x = 3^{10} \bmod 13$

(D) $x = 7^{100} \bmod 13$

(E) $7^x = 11 \bmod 13$ (Discrete Logarithm Problem. We will talk in detail in Chapter 8)