

Overleaf Homework Template

Question 1. Write down sets in order of containment.

We pretend that equivalence classes are just numbers.

$$\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \supset \mathbb{Z} \supset \mathbb{N} \supset \mathbb{P} \not\supset (\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}) \supset \{\emptyset\}$$

Question 2. Find roots of $x^2 - 8x = 9$.

We proceed by factoring,

$$\begin{aligned} x^2 - 8x - 9 &= 9 - 9 \\ x^2 - x + 9x - 9 &= 0 \\ (x - 1)(x + 9) &= 0 \\ x &\in \{1, -9\} \end{aligned}$$

Subtract 9 on both sides.

Breaking the middle term.

Pulling out common $(x - 1)$.

$$f(x)g(x) = 0 \Rightarrow f(x) = 0 \vee g(x) = 0.$$

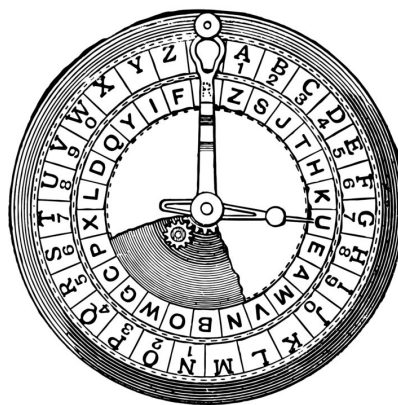
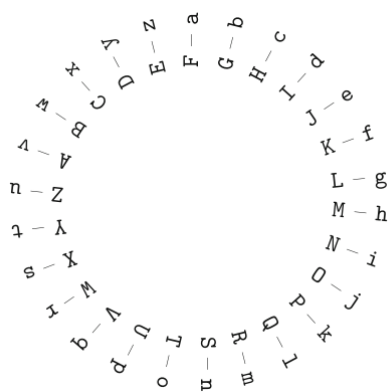


FIGURE 1. Cipher wheels.

Question 3. Figure 1 shows two cipher wheels. The left one is from Jeffrey Hoffstein, et al. [1] (pg. 3). Write a Python 3 program that uses it to encrypt: FOUR SCORE AND SEVEN YEARS AGO.

```

1 def encrypt(plain):
2     cipher = ''
3     for c in plain:
4         cipher = cipher+c if c==' ' else cipher+chr(((ord(c)-60) % 26)+65)
5     return cipher
6 print(encrypt("FOUR SCORE AND SEVEN YEARS AGO"))

```

LISTING 1. Python 3 implementing figure 1 left wheel.

We get: KTZW XHTWJ FSI XJAJS DJFWX FLT.

REFERENCES

- [1] Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman, and Joseph H Silverman. *An introduction to mathematical cryptography*, volume 1. Springer, 2008.