September 15, 2025

Problem Set 2

Exercise 1. Recall that the Euler's totient function $\varphi(n)$ is defined for any $n \in \mathbb{Z}^+$ as the number of positive integers smaller than n, that are coprime to n.

(a) Show that $\varphi(p^k) = p^k - p^{k-1}$, where p is a prime and $k \in \mathbb{Z}^+$.

(b) Show that $\varphi(p_1 p_2) = (p_1 - 1)(p_2 - 1)$, where $p_1 \neq p_2$ are two distinct primes.

(c) Compute $\varphi(n)$ for all natural $n \leq 20$.

(d) Assuming that for any $a, b \in \mathbb{Z}^+$ such that $\gcd(a, b) = 1$ $\varphi(ab) = \varphi(a)\varphi(b)$ (we will prove this later), derive a formula for $\varphi(n)$ in terms of the prime factorization of n.

(e)* Let $m_n = p_1 p_2 \dots p_n$ denote a product of the first n primes. Show that

$$\lim_{n\to\infty} \frac{\varphi(m_n)}{m_n} = 0.$$

Hint: Use the fact that $\displaystyle\sum_{i=1}^{\infty} \frac{1}{p_i}$ is divergent.

Exercise 2. Recall that for an RSA encryption we need a number N that is a product of two large distinct primes and an encryption key e such that $\gcd(e, \varphi(N)) = 1$, where $\varphi(N)$ is the Euler totient function of N. Any number M in the set $\{1, 2, \dots N\}$ can be encoded by computing $C = M^e \pmod N$. The decryption key consists of a number d such that $ed \equiv 1 \pmod{\varphi(N)}$. We have proved in class that if we know d, we can decode the original message M as $M = C^d \pmod N$. For this exercise suppose that $N = 527$ and $e = 17$.

(a) Encode the message $M = 113$.

(b) Encode the message $M = 500$.

(c) This RSA example has weak security because the number N is small. Break the RSA by factoring N and finding $\varphi(N)$ and d.

(d) Using the value of d found above, decode the message $C = 3$.

(e) Check that for C found in (a), you have $C^d \equiv 113 \pmod{527}$, so that indeed you can recover the original message.

Exercise 3. Show that the set B of all matrices of the form

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}, \quad a, b \in \mathbb{R}, \ \ a \neq 0$$

is a group with respect to the matrix multiplication.
Consider the following subsets in B:

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\}_{a\neq 0} \quad U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}_{b\in\mathbb{R}} \quad K = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \right\}_{a>0, b\geq 0}$$

Which of D, U, K are subgroups of B?

Exercise 4. Consider the transformations in $\mathbb{R}^2$ given by the matrices

$$S_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad S_1 = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

Check that $S_0^2 = 1$ and $S_1^2 = 1$. Let G be the group generated by S_0 and S_1. Find all elements of G and write down a multiplication table between them.

Hint: Since $S_0^2 = S_1^2 = 1$, the only nontrivial elements in G are the products where S_0 and S_1 alternate. Find all distinct elements of this form and determine their products.