Problem Set 2

Basic Arithmetics

Problem I

1. Use the Euclid Algorithm[1] to compute the Greater Common Divisor of 2008 and 1757.

2. Decompose 2008 and 1757 as a product of prime numbers. Deduce the Greater Common Divisor and compare the result to the previous question.

3. Compute the Least Common Multiple of 2008 and 1757.

Problem II

Find two integers x and y such that

$$17x + 19y = 1$$

Are x and y unique?

Problem III

Can you find two integers x and y such that $6x + 8y = 1$?

Problem IV

Use the following algorithms to test the primality of 137

1. Erathostene sieve

2. Fermat

3. Miller-Rabin

[1] Euclid of Alexandria, Greek mathematician from the third century BC, is considered the father of geometry. In his *elements*, the principles are deduced from a small set of axioms. Euclid was also involved with perspective, conic sections and spherical geometry.

Euclid of Alexandria ($\sim$ 365-300 BC)

Problem V

Let φ be the totient function.

1. Compute $\varphi(199)$.

2. Compute $\varphi(583)$.

Problem VI

1. Prove that

$$n \text{ is prime} \iff \mathbb{Z}/n\mathbb{Z} \text{ is a field}$$

2. Let φ be the totient function and $n \in \mathbb{N} \setminus \{0, 1\}$. Prove that

$$n \text{ is prime} \iff \varphi(n) = n - 1$$

Problem VII

Find the inverse of 9 modulo 25.