PRIMITIVE ROOTS

ANTONELLA PERUCCA AND TIM SEURÉ

Primitive roots are key to modular arithmetic.
Modular arithmetic is key to cryptography.

We are glad to offer you a very accessible topic which is also a subject of modern research. The aim of the project is collecting and analysing data related to primitive roots modulo prime numbers. Let us be more precise.

Recall that if p is a prime number, then a *primitive root* modulo p is an integer a such that a^{p-1} is the smallest power of a that is congruent to 1 modulo p. It can be shown that there are primitive roots modulo p for every prime p.

Unfortunately, no general formula exists that takes p as an input and outputs a corresponding primitive root. Instead, one makes use of algorithms to find such primitive roots. The goal of this project is to collect data which may help speed up these algorithms. For instance, given a prime number p, an interesting first step would be to experimentally find the smallest positive integer n for which either $+n$ or $-n$ is a primitive root modulo p.

Prerequisites: It would be convenient to have already seen congruences, meaning the basics of modular arithmetic. It would also be useful to have some basic programming skills (Python, SageMath, ...), but if not, this project will let you acquire them.

EML Project for any semester - Bachelor Thesis - Master Thesis
(Teamwork for up to 4 people)