Proseminar/Seminar: Prime numbers and Cryptography

Dr. B. S. Banwait, C. V. Sriram SS 2022

Prime numbers are among the most basic objects in mathematics, and were studied by several ancient civilisations such as the Egyptians, the Indians, and the Greeks. Although arising from pure mathematics, in recent history they have seen crucial application through the study of Cryptography. The encoding and decoding of secret messages was a major part of the war efforts of both the Allied and Axis powers during the Second World War. Today prime-number-based cryptographic systems form the basis of the SSL protocol (the 'S' in 'HTTPS') and are thereby responsible for virtually all encrypted internet traffic; as such we all use this tools frequently when sending emails or making online payments.

This seminar will develop the theory that lies behind these real-world applications, via a hands-on, algorithmic approach: Fast arithmetic in $\mathbb{Z}/n\mathbb{Z}$, complexity analysis, and probabilistic methods as well as the number field sieve, a technique arising from algebraic number theory. Elliptic curve analogues will also be seen. The specific themes are as follows (references to the book *Prime numbers - A computational perspective* by Crandall and Pomerance), * denotes suitablility also as Bachelor seminar talk:

1. Complexity analysis, Examples §2+3
2. Fast Arithmetic: DFT, Schönhage-Strassen §9 (two talks)
3. Psueodprimes and Miller-Rabin §§3.3-3.5
4. Mersenne numbers and the Lukas-Lehmer test §4.2
5. AKS-Test: 'PRIMES is in P' (two talks)
6. Prime Factorisation I: Pollard-Rho and Baby-Step-Giant-Step §5
7. Prime Factorisation II: smooth numbers and the quadratic sieve §6.1

8.* Prime Factorisation III: The number field sieve §6.2 (two talks)

9.* Elliptic curves

10.* Public-key cryptosystems §8.1

11.* Elliptic curve factoring algorithms §§7.4, 7.6

12.* Post-quantum cryptography and Supersingular Isogeny Diffie-Hellman.

When? This is a **Block seminar**: all talks will take place from **April 11$^{\text{th}}$ - 14$^{\text{th}}$ 2022** inclusive.

Vorbesprechung: Wednesday 16$^{\text{th}}$ February 2022 at 2pm (ct) in INF 205/HS (Großer Hörsaal). Please register your interest in **Müsli**.

Prerequisites: Lineare Algebra 2 (expected), Algebra 1 (desirable)

Course Website: `https://typo.iwr.uni-heidelberg.de/groups/arith-geom/members/barinder-banwait/prime-numbers-and-cryptography-proseminar`

Contact: barinder.banwait@iwr.uni-heidelberg.de.