PROSEMINAR/SEMINAR: PRIME NUMBERS AND FACTORISATION IN CRYPTOGRAPHY

DR. B. S. BANWAIT AND C. V. SRIRAM

1. Introduction

While it has long been known that there are infinitely many prime numbers, the precise distribution of the primes in the set of natural numbers remains a major open problem; indeed it could be said that this is equivalent to the famous Riemann Hypothesis!

An easier question is that of testing whether a given integer n is prime or not. Trial division with all integers less than n quickly becomes inpractical as n grows. Only since 2002 has there been a fast and reliable algorithm - the Agrawal-Kayal-Saxena (AKS) algorithm - which satisfactorily resolves this. Namely, if n is a given integer with D digits, the AKS algorithm will determine whether or not n is prime in "about D^6 steps"; i.e. in *polynomial time.* One of the main goals of this seminar is to formalise this notion of "about D^6 steps" and to explain the ideas of modular arithmetic and fast multiplication upon which the AKS algorithm is based.

Before we treat the AKS-algorithm in detail, we begin with some probabilistic methods for primality testing, which often work in practice and which are extremely fast. In particular, a method to test primality of numbers of the form $2^q - 1$ will be given.

Trial division does have one important advantage in comparison to the above mentioned tests: it actually provides an explicit divisor of n in the case it is not prime. Nevertheless for this question of finding divisors there are much faster methods which fall under the umbrella term of *sieving*; these will be discussed in the second half of the seminar. It is still an open question if one can find a divisor of n in polynomial time.

The difficulty of prime factorisation may be expressed as saying that multiplication of two large prime numbers is a 'one-way function': easy to compute, difficult to reverse. As such, this becomes an important tool in Cryptography, which is the focus of the last part of the talk. Since modern day cryptosystems are based on the theory of elliptic curves, a quick overview of what is required will be given, before discussing several important cryptosystems such as ECDH and RSA. The last talk will give a very recent example of a *post-quantum cryptosystem*, one that is expected to be secure even against computational attack; this is the subject of much active research in Cryptography.

2. Practicalities

1. **Prerequisites.** Students are expected to have successfully completed Lineare Algebra 2. Algebra 1 would be helpful but is not necessary.

barinder.banwait@iwr.uni-heidelberg.de.
sriram.chinthalagiri@iwr.uni-heidelberg.de.

2. **Seminar Format.** This is a **Block seminar**; all talks will take place in the four days **April 11th - 14th 2022** inclusive. Students interested in participating in this seminar will meet on **Wednesday 16th February 2022** at 14 Uhr (ct) in INF 205/HS (the big Hörsaal). The talks will be allocated in this session.

Students will then be expected to independently study the material and prepare for their talk. They will be able to ask the course instructors questions and for guidance and clarifications of any doubts, during office hours to be arranged.

Every speaker will then meet one or both course instructors in the week **March 28th - April 1st 2022** to ensure the student has a firm grasp of the material of their talk. Ideally the material of the talk will be firmly understood by this point. Both course instructors are happy to answer questions before this via email or in-person.

Students will then have the week before the seminar - **April 4th - April 8st 2022** - for the final preparation. The handout of the talk must also be submitted in this week.

Note that the last 6 talks of this course are also suitable as Bachelor seminar talks.

3. **Requirements of the participants.**

(1) **Delivery of seminar talk**. The student is expected to deliver a 90-minute talk on their chosen topic. Definitions and results must be stated clearly, and where possible illustrated with concrete examples. Ideally the student will have worked through and understood all proofs; some of these proofs should be presented, though for reasons of time others may have to be omitted.

(2) **Preparation of handout**. The student is expected to prepare a handout for the other participants containing a summary of their talk, and highlighting the most salient aspects of it.

(3) **Timelines for preparation of talk and handout**.

   (a) As stated above every speaker will meet one or both course instructors in the week March 28th - April 1st 2022 to discuss the proposed talk and to identify any points of confusion.

   (b) The handout is to be submitted in the week April 4th - April 8st 2022, to Dr. Banwait.

(4) **Mode of delivery**. Talks will be delivered in person to the other participants of the seminar, either on the chalkboard or with a Beamer or slideshow presentation.

(5) **Language of talk and handout**. Both the talk as well as the handout are expected to be in English.

4. **Student Evaluation.** Students will be evaluated based on the clarity of both the talk as well as the handout.

3. Talks

Unless otherwise stated references are to the book of Crandall and Pomerance [CP05].

1. **Prime numbers and Complexity analysis.** Definition of a prime number. The Fundamental Theorem of Arithmetic (1.1.1). Basics on modular arithmetic, and the extended Euclidean algorithm. Quadratic residues and the symbols of Legendre and Jacobi. Statement of Quadratic reciprocity (Thm 2.3.4 - proof not required). Fast computation of Jacobi symbols (Algorithm 2.3.5). O/o notation (§1.1.4). Extended Euclidean Algorithm and computation of Jacobi symbols are polynomial time. Definition of $\pi(x)$ (§1.1.3), the prime number theorem (Thm 1.1.4), the Riemann zeta function and its Euler product decomposition (Thm 1.4.1).

2. **Fast arithmetic I : Fourier Transform Algorithms.** Base B representation of an integer, and complexity of "grammar-school multiplication" (§9.1.1). The Discrete Fourier Transform (§9.5.2) and the Fast Fourier Transform (§9.5.4).

3. **Fast arithmetic II : Complexity of multiplication algorithms.** Overview of Schönhage and Nussbaumer methods (§9.5.6 and 9.5.7 - technical details not required). Comparison of complexity of some multiplication algorithms (§9.5.8). Exponentiation via ladders (§9.3.1), and square roots via Newton's method ((§9.2.2 and Algorithm 9.2.11).

4. **Pseudoprimes and the Miller-Rabin test.** Infinitude of Fermat Pseudoprimes (Theorem 3.3.4). Infinitude of Carmichael numbers (Theorem 3.3.7, statement only). The material from §3.5. Probable primes and witnesses. The Miller-Rabin test (Algorithm 3.5.2) and "Indisutrial-grade prime" generation" (Algorithm 3.5.7). (Lemmas at the end of the section may be stated without proof.)

5. **The Theorem of Agrawal-Kayal-Saxena I.** This talk will present the first three sections of the article of Granville [Gra05]. Child's Binomial Theorem, Fermat's Little theorem, and the definition of `P` and `NP` classes. Statement of the theorem of Agrawal-Kayal-Saxena.

6. **The Theorem of Agrawal-Kayal-Saxena II.** This talk will present the proof of the Agrawal-Kayal-Saxena theorem, given in §4 of [Gra05]. Time permitting the improvement of Lenstra and Pomerance (§7) can be presented.

7. **Factorisation I - Pollard-Rho method and Baby-Step-Giant-Step.** Pollard's ρ-method (§5.2.1). The discrete logarithm problem in a cyclic group (§5.2.2), the Baby-Step-Giant-step method, and complexity analysis (§5.3). time permitting, the Lambda algorithm (§5.2.3).

8. **Factorisation II - Smooth numbers and the quadratic sieve.** Definition of smooth numbers. The sieve of Eratosthenes. Applications of sieving, and practical considerations. The quadratic sieve This is based on §§3.3-3.4 and §§6.1.1-6.1.2.

The following six talks are suitable for delivery as Bachelor seminar talks as well as Proseminar talks.

9. **Brief overview of Algebraic number theory.** This will be a collection of key facts from the realm of number fields and algebraic number theory, with few proofs, and many examples illustrating the theory. The topics will be as follows.

Definition of number field. Notion of integrality, and the ring of integers. Definition of Dedekind domains. Ideals and lattices. Difference between prime and irreducible elements. Failure of uniqueness of factorisation of some rings of integers. The class number. Dirichlet's unit theorem.

References: [Neu06], Chapter 1, Sections 1–7.

10. **Factorisation III - The number field sieve.** Basic Number field sieve. Strategy. Exponent vectors. Complexity. Obstructions. Square roots, Summary algorithm. Further considerations. This is all based on §6.2.

11. **Brief overview of elliptic curves.** Definition of elliptic curves over finite fields (§7.1). Some practical algorithms for elliptic curve arithmetic (§7.2 up to and including Definition 7.2.5). Supersingular and ordinary elliptic curves. (Theorem 3.1 in Chapter V Section 3 of [Sil09]) The theorems of Hasse, Deuring and Lenstra (§7.3).

12. **Public-key cryptography.** Diffie-Hellman key exchange. The RSA cryptosystem. Digital signature algorithms. Elliptic curve analogues of the above. The coin-flip protocol.

References: §8.1 of [CP05]; see also the original article of Diffie-Hellman [DH76].

13. **Lenstra's elliptic curve method and elliptic curve primality proving.** Lenstra's elliptic curve method. Elliptic curve primality proving.

References: §§7.4, 7.6. For interest see also Lenstra's original article [Jr87].

14. **Post-quantum cryptography, and the Supersingular Isogeny Diffie-Hellman protocol.** Brief non-technical remarks on quantum computers and their compromising of existing cryptosystems. The need for 'quantum-secure cryptosystems'. Isogenies between elliptic curves. Isogeny graphs of elliptic curves over finite fields. Cryptography from random walks on expander graphs. Hard homogeneous spaces and the Supersingular Isogeny Diffie-Hellman protocol of Jao and De Feo.

References: §§2, 9, 11, 14 of [Feo17].

References

[CP05] Richard Crandall and Carl Pomerance. *Prime numbers - A computational perspective.* Springer, 2005. available online at `http://thales.doa.fmph.uniba.sk/macaj/skola/teoriapoli/primes.pdf`.

[DH76] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[Feo17] Luca De Feo. Mathematics of isogeny-based cryptography. available at `https://arxiv.org/pdf/1711.04062.pdf`, 2017.

[Gra05] Andrew Granville. It is easy to determine whether a given integer is prime. *Bulletin of the American Mathematical Society*, 42(1):3–38, 2005.

[Jr87] Hendrik W Lenstra Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987.

[Neu06] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer-Verlag, 2006.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

Email address: barinder.banwait@iwr.uni-heidelberg.de

Email address: sriram.chinthalagiri@iwr.uni-heidelberg.de