Number Theoretic Algorithms

1. RSA and factorization

1. Describe an oracle-based factorization algorithm for determining an RSA private key (Alg 1). Prove its correctness and estimate the probability of success. (1.3, 1.4).

2. Pollard's ρ-method

2. Describe and explain the factorization Pollard-Floyd algorithm (Alg 4) using related notions and their properties. (2.1, 2.5).

3. B-powersmooth numbers

3. Introduce the nothins of B-smooth and B-powersmooth numbers, and describe the first version of Pollard's (p-1) factorization algorithm (Alg 5A). What is its time complexity? (3.5)

4. Write the 2nd version of Pollard's (p-1) algorithm (Alg 5B) and prove the probability of success for factoring the product of two prime numbers (3.7).

5. Write and briefly explain the factorization (p+1)-method (Alg 6). (3.9)

4. Lenstra's elliptic-curve algorithm

6. Explain the principles (without proof) of Lenstra's ECM algorithm .

7. Briefly explain the principles of Lenstra's ECM algorithm (Alg 8) and prove the statement regarding its success (4.3).

5. Roots modulo n

8. Write the Tonelli-Shanks algorithm for computing the square root modulo an odd prime number, and explain its correctness and time complexity (Alg 10). (5.2)

9. Write algorithms for computing the roots of a second-degree polynomial and a general polynomial modulo an odd prime number (Alg 11, 12).

10. Describe and explain the algorithm for taking the square root modulo a power of a prime (Alg 13). (5.3)

11. Describe an attack on RSA using a deterministic oracle to compute the square root modulo the product of two distinct prime numbers (Alg 14), and prove the statement regarding its correctness and the probability of failure (5.5).

6. Dixon's faktorization and CFRAC

12. Introduce the notions of factorization bases, relations, and smooth relations, and write down the scheme for Dixon factorization. How does its linear phase work? (formulation of 6.2)?

13. Formulate the algorithm for computing the power series expansion of the square root $\sqrt{N}$ using a single approximation $\lfloor\sqrt{N}\rfloor$ (Alg 16) and prove its correctness (6.5).

14. Formulate the CFRAC factorization algorithm using continued fractions (Alg 17) and prove its correctness (6.7).

7. Quadratic sieve

15. Describe the relation generator for the quadratic sieve (including a description of the relations themselves) and formulate one of the sieving variants (Alg 18A, 18B, or 18D).

8. Discrete logarithm

16. Formulate and prove the statement regarding the Pohlig-Hellman reduction of the discrete logarithm problem to the discrete logarithm problem for its divisors. How does the Baby-steps, giant-steps algorithm (Alg 19) work? (8.1).

17. Describe the oracle factorization algorithm for solving the generalized discrete logarithm problem in the group Z_N^* (Alg 20), and briefly explain (by referring to relevant assertions; no proof is required) its correctness and probability of success (formulation of 8.2, 8.3).