

Programm für einen zweisemestrigen Kurs

“Algorithmische Zahlentheorie und Elemente der Kryptographie”

(Leiter: Prof. Dr. Oleg V. Bogopolski)

Zahlentheorie und Algebra spielen eine wachsende und signifikante Rolle für Informatik und Wissensvermittlung. Dies ergibt sich auch aus ihrer Anwendung im Bereich der Kryptographie und Kodierung. Das Ziel der Vorlesung ist eine Einführung in die Zahlentheorie und Algebra mit Anwendungen besonders in der Kryptographie. Der Schwerpunkt soll dabei auf Algorithmen und ihren Handlungen liegen.

Diese Vorlesung ist Studierenden der Fächer Informatik und Mathematik zu empfehlen, die in vorausgegangenen Kursen schon ein generelles mathematisches Grundlagenwissen erworben haben, aber noch nicht über allzu viele spezielle mathematische Kenntnisse verfügen. Diese Vorlesung ist auch für Lehramtstudierende (Bereich Algebra und Zahlentheorie) und für angehende Wirtschaftsmathematiker geeignet. Eine Fortsetzung im WS 2006/07 ist geplant.

1. Euklidischer Algorithmus. Laufzeitanalyse: Satz von Lamé. Kongruenzen.
2. Gruppen und Ringe. Restklassenring modulo n . Chinesischer Restsatz und seine Anwendungen.
3. Grundlagen der Gruppentheorie: zyklische Gruppen, Ordnung des Elementes, Untergruppen, der Satz von Lagrange.
4. Grundlagen der Körpertheorie. Endliche Körper. Euler'scher Satz, kleiner Fermatischer Satz.
5. Struktur der multiplikativen Gruppe des Restklassenringes modulo n .
6. Ring des Polynomes. Diskrete Fourier-Transformation. Ein Algorithmus für schnelle Multiplikation des Polynomes.
7. Quadratische Reste. Legendre-Symbol und Jacobi-Symbol. Quadratisches Reziprozitätsgesetz.
8. Diskreter Logarithmus. Algorithmen zur Berechnung des diskreten Logarithmus: Babystep-Gaintstep-Algorithmus, Pohlig-Hellman-Algorithmus, Index-Calculus-Algorithmus, Pollard-Rho-Methode. Anwendungen: Einwegfunktionen in der Kryptographie. Diffie-Hellman-Schlüsselaustausch.
9. Verteilung der Primzahlen. Zwei Sätze von Tschebyschow über Primzahlen.
10. Allgemeine Struktur der probabilistischen Primzahltesten. Fermatischer Primzahltest. Carmichael-Zahlen. Starke pseudoprimzahlen. Miller-Rabin-Primzahltest.

11. Komplexitätstheorie. Turingmaschinen. Sprachen. Komplexitätsklassen \mathcal{P} und \mathcal{NP} . \mathcal{NP} -vollständigen Problemen.
12. Polynomielle deterministische Primzahl-Algorithmus von Agrawal, Kayal and Saxena.
13. RSA-Kryptosystem.
14. Berechnungen in den Ringen von Polynomen. Algorithmen von Berlekamp und Cantor-Zassenhaus. Anwendungen in der Kodierungstheorie.

Literatur

- [1] E. Bach and J. Shallit, *Algorithmic number theory*, v. I: Efficient algorithms, MIT Press, Cambridge - Massachusetts, 1996.
- [2] A. Granville, *It is easy to determine whether a given integer is prime*, Bulletin of the American Math. Soc., v. 42, N 1, 3-38.
- [3] J.E. Hopcroft, R. Motvani, J.D. Ullman, *Introduction to automata theory, languages and computations*, 2-nd ed, Williams Publishing House, 2002.
- [4] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, Cambridge, 2005. Available on the website <http://www.shoup.net/ntb>.
- [5] N. Smart, *Cryptography: an introduction*, McGraw-Hill Education, 2002.
- [6] I.M. Vinogradov, *Introduction to the number theory*, Dover Publications, New York, 2003 (Translated from Russian: Introduction to the number theory, 5th ed., Moscow, Gostechizdat, 1952.)
Deutsche Aufgabe: I.M. Winogradow, *Elemente der Zahlentheorie*, Verlag R. Oldenburg, München, 1956. (Der Übersetzung liegt die 6. Auflage des Originalwerkes [Moskou, Verlag Gostechisdat, 1952] zugrunde.)
- [7] V.V. Yaschenko (ed.) *Cryptography: an introduction.*, AMS Series: Student Math. Library, v. 18, 2002.