Programm des Seminars über Zahlentheorie

Prof. Dr. Irene Bouw
Christian Steck, Michael Eskin
Universität Ulm
Institut für Reine Mathematik
WS 2013/14
irene.bouw@uni-ulm.de

Vortrag 1: Definition und Eigenschaften von Kettenbrüche

- Definieren Sie endliche und unendliche Kettenbrüche.
- Beschreiben Sie den Algorithmus zur Berechnung der Kettenbruchentwicklung einer reellen Zahl, [14, §. 12.2, § 12.3]. Geben Sie auch Beispiele.
- Diskutieren Sie kurz die Charakterisierung periodischer Kettenbrüche ([14, §. 12.4]).

Vortrag 2: Faktorisieren mit Hilfe von Kettenbrüchen

- Beschreiben Sie die Fermat-Methode zum Faktorisieren von ganzen Zahlen ([4, §. 5.1+5.2]).
- Beschreiben Sie die Kettenbruchentwicklung von $\sqrt{n}$, [14, Theorem 12.22].
- Beschreiben Sie die Kettenbruchmethode zum Faktorisieren ganzer Zahlen (Morrison-Brillhart-Algorithmus), [14, §. 12.5]. Siehe auch [13].

Vortrag 3: Die Pellsche Gleichung

- Stellen Sie die Pellsche Gleichung vor. Erklären Sie auch einige der historischen Hintergründe ([9], [10, History topic: Pell's equation]).
- Erklären Sie [14, Theoreme 13.10, 13.11, 13.12] und geben Sie auch Beispiele.

Vortrag 4: Die Fibonaci-Zahlen

- Definieren Sie die Folge der Fibonaci-Zahlen.

- Erklären Sie den Zusammenhang zur Kettenbruchentwicklung des goldenen Schnitts ([15, Seite 62]).
- Beweisen Sie die Darstellung in [15, Satz 34].
- Erklären Sie die Laufzeitabschätzung des euklidischen Algorithmus ([15, Satz 33].

Vortrag 5: Digitale Unterschriften

- Erklären Sie das Konzept der digitalen Unterschrift, [8, § 7.1], [3, Kapitel 5]. Finden Sie alltägliche Anwendungen. Diskutieren Sie auch welche Anforderungen man an ein gutes Signaturverfahren stellen sollte.
- Beschreiben Sie die RSA- und ElGamal-Signaturverfahren. Erklären Sie auch die Rolle des kurzlebigen Schlüssels e ([8, § 7.2+7.3], [3, §. 5.2+5.3]).
- Beschreiben Sie das DSA-Verfahren. Erklären Sie auch die Vorteile. Das DSA-Verfahren benutzt die Existenz einer Primitivwurzel mod p. Der Zusammenhang soll erklärt werden.
- Interessant wäre es auch Varianten wie blinde oder nicht-abstreitbare Unterschriften zu diskutieren ([3, §. 5.4]).

Vortrag 6: Primzahltests I

- Definieren Sie die Fermat-Primzahlen. Beweisen Sie [7, Theorem 1.3.4, Theorem 1.3.5]. (Siehe auch http://primes.utm.edu/glossary/xpage/FermatNumber.html).
- Beschreiben Sie den Lucas- und den Pepin-Primzahltest ([7, §. 4.1.1], [11, Satz 11.3+11.6]).

Vortrag 7: Primzahltests II

- Wiederholen Sie quadratische Reste und definieren Sie das Legendre- und das Jacobi-Symbol ([2, §. 7.1+7.3]).
- Definieren Sie Carmichael-Zahlen ([2, Def. 3.3.5]). Erklären Sie auch die Relevanz bei der Bestimmung ob eine gegebene Zahl eine Primzahl ist.

- Erklären Sie den Solovay-Strassen-Primzahltest ([11, Satz 11.12]).
- Erklären Sie den Unterschied zwischen deterministischen und probabilistischen Primzahltests und diskutieren Sie dies für den Solovay-Strassen-Primzahltest ([11, Seite 88-89]).

Vortrag 8: Pseudoprimzahlen

- Beweisen Sie [7, Thm. 3.6.1] und definieren Sie Fibonacci-Pseudoprimzahlen ([7, Def 3.6.2]. Vergleichen Sie diese Definition zur Definition von Pseudoprimzahlen in [2, Def. 3.3.1].
- Beschreiben Sie die Verallgemeinerung der Lucas-Pseudoprimzahlen ([7, Thm. 3.6.3+Def. 3.6.4]). (Die Fibonacci-Zahlen wurden im Vortrag 4 beschrieben, siehe [15, Satz 34].)

Vortrag 9: Das Münzwurfprotokoll

- Erklären Sie den Algorithmus von Tonelli und Shanks zur Berechnung von Quadratwurzeln modulo p für Primzahlen $p \equiv 3 \pmod 4$, [12, §. 3.4.1], [3, Lemma 7.2.3].
- Sei $n = pq$ mit $p \neq q$ zwei Primzahlen $p, q \equiv 3 \pmod 4$. Diskutieren Sie das Problem der Bestimmung von Quadratwurzeln mod n ([3, Lemma 7.2.1]).
- Beschreiben Sie das Protokoll, [1], [3, §. 7.2].

Vortrag 10: Pythagoräische Tripel

- Formulieren Sie Fermats letzen Satz. Erklären Sie auch etwas zu den Hintergründen ([10, History Topic: Fermat's last Theorem]).
- Definieren Sie Pythagoräische Tripel (PT). Beschreiben Sie alle PTs ([2, Theorem 7.1.4, Lemma 7.1.5]).
- Benutzen Sie dies um Fermats letzten Satz für $n = 4$ zu beweisen. ([2, Thm. 7.1.6, Kor. 7.1.7]).

Vortrag 11: Summe von zwei Quadraten

- Definieren Sie den Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen ([2, Def. 7.3.1]). Erklären Sie den Euklidischen Algorithmus in $\mathbb{Z}[i]$ ([2, Satz 7.3.4]). Insbesondere existieren ggTs in $\mathbb{Z}[i]$.

- Zeigen Sie, dass eine Primzahl genau dann als Summe von zwei Quadraten geschrieben werden kann, wenn $p \not\equiv 3 \pmod 4$. ([11, Satz 9.1]). Beschreiben Sie auch [11, Kor. 9.2]) und geben Sie Beispiele.

Vortrag 12: Kongruente Zahlen

- Definieren Sie, was eine kongruente Zahl ist und geben Sie Beispiele. Erklären Sie auch den Zusammenhang zu den Pythagoräischen Tripeln ([6]).

- Zeigen Sie, dass 1 keine kongruente Zahl ist ([6, Theorem 2.1].

- Beschreiben Sie den Zusammenhang zwischen kongruenten Zahlen und Lösungen der Gleichung $y^2 = x^3 - n^2x$ ([6, §. 4]).

Literaturverzeichnis

[1] M. Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15(1):23-27, 1983. http://portal.acm.org/citation.cfm?doid=1008908.1008911

[2] I.I. Bouw, *Elementare Zahlentheorie*. Vorlesungsskript, 2010.

[3] I.I. Bouw, *Kryptologie*, Vorlesungsskript Somersemester 2012.

[4] D. Bressoud, *Factorisation and primality testing*. Undergrad. Texts in Math. Springer, 1998.

[5] J. Buchmann, *Einführung in die Kryprographie*. 3. Auflage.

[6] K. Conrad, The congruent number problem. http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/congnumber.pdf

[7] R. Crandall, C. Pomerance, *Prime numbers, a computational perspective*, Springer 2005.

[8] J. Hoffstein, J. Pipher, J. Silverman, *An introduction to mathematical Cryptography*. Undergrad. Texts in Math., 2008.

[9] H.W. Lenstra Jr., Solving the Pell equation, *Notices of the AMS*, Vol. 49, 2, February 2002, http://www.ams.org/notices/200202/fea-lenstra.pdf

[10] The MacTutor History of Mathematics archive, http://www-history.mcs.st-and.ac.uk/

[11] S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie* , Vieweg 2006.

[12] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of applied cryptography*, http://www.cacr.math.uwaterloo.ca/hac/

[13] C. Pomerance, A tale of two sieves, *Notices of the AMS*, Volume 43, 12, December 1996, http://www.ams.org/notices/199612/pomerance.pdf

[14] K. Rosen, *Elementary number theory and its applications*.

[15] H. Scheid, A. Frommer, *Zahlentheorie*, 4. Auflage, Spektrum, 2007.