Proseminarprogramm Sommersemester 2019

Primzahlen

Voraussetzungen

Lineare Algebra 1

Vorbesprechung und Themenvergabe

Die Vorbesprechung findet am 6. 2. 2019 um 13 Uhr s.t. in Seminarraum 4 des Mathematikon INF 205 statt. Hier werden auch die Vortragsthemen vergeben.

Vorträge

Vortrag 1: Algebraische Grundlagen **(26. 4. 2019)**

Wir erinnern an Äquivalenzrelationen und zeigen den Homomorphiesatz für Ringe. Anschließend definieren wir für eine natürliche Zahl n den Ring $\mathbb{Z}/n\mathbb{Z}$ als Quotientenring der ganzen Zahlen und untersuchen einige seiner Eigenschaften. Wir erinnern an den Begriff des Ideals, bestimmen die Ideale in $\mathbb{Z}$ und lernen die Begriffe „Hauptidealring“ und „faktorieller Ring“ kennen.

Quelle: Ein beliebiges gutes Lehrbuch der Linearen Algebra oder Algebra. Bitte mit mir absprechen!

Vortrag 2: Der erweiterte euklidische Algorithmus **(3. 5. 2019)**

Zunächst wollen wir an den bekannten euklidischen Algorithmus in den ganzen Zahlen $\mathbb{Z}$ erinnern. Diesen wollen wir im Folgenden gleich in mehrerlei Hinsicht verallgemeinern: Zum einen führen wir das Konzept des euklidischen Rings ein und zeigen, dass der bekannte Algorithmus auch in dieser Allgemeinheit funktioniert. Zum anderen erweitern wir den Algorithmus dahingehend, dass wir mehr Information speichern, so dass wir den ggT zweier Elemente eines euklidischen Rings R als Summe von R-Vielfachen dieser Elemente ausdrücken können. Auf diese Weise zeigen wir, dass Ideale in euklidischen Ringen immer schon von einem Element erzeugt werden, was uns auf das Konzept des Hauptidealrings führt.

Quelle: Abschnitte 3.1 und 3.2 in [GG] und 2.2 in [Bos], wobei dort der Satz, dass $\mathbb{Z}$ ein Hauptidealring ist, durch das allgemeinere Korollar 3.9 aus [GG] und die Implikation, dass euklidische Ringe Hauptidealringe sind, ersetzt werden soll. Es bietet sich an, die Euklidizität in einem Beispiel zu zeigen; das soll mit den ganzen Gauß'schen Zahlen $\mathbb{Z}[i]$ geschehen. Ein Beweis ist in Abschnitt 2.4 von [Bos] skizziert.

Vortrag 3: Aufwandsberechnung und Anwendung des euklidischen Algorithmus (10. 5. 2019)

Zu Beginn erinnern wir an die Landau-Notation und führen die Komplexitätsklassen $\mathcal{P}$ und $\mathcal{NP}$ ein. Damit haben wir das Handwerkszeug, um eine Aufwandsberechnung für den im letzten Vortrag eingeführten erweiterten euklidischen Algorithmus über $\mathbb{Z}$ und über dem Polynomring $K[X]$ über dem Körper K durchzuführen. Parallel zu den aus der Linearen Algebra bekannten Restklassenringen $\mathbb{Z}/n\mathbb{Z}$ führen wir Restklassenringe R/I in beliebigen Ringen R ein. In diesen, und damit insbesondere in endlichen Körpern, können wir nun mit dem euklidischen Algorithmus Inverse von Einheiten berechnen.

Quelle: Abschnitte 3.3, 4.2 (bis inklusive Example 4.3) und 25.7 von [GG]. Es empfiehlt sich, auch die Paragraphen 2.3, 2.4, 4.1 und 25.8 zu überfliegen. Die Konstruktion der Restklassenringe geht exakt wie die im Spezialfall $R = \mathbb{Z}$, soll im Vortrag aber ausgearbeitet werden.

Vortrag 4: Endliche Körper (17. 5. 2019)

Wir nutzen das Verfahren aus dem letzten Vortrag, um Körpererweiterungen zu konstruieren, zuerst noch allgemein, dann speziell für $\mathbb{F}_p$ als Grundkörper. Wir zeigen, dass euklidische Ringe und insbesondere $K[X]$ faktoriell sind (und sagen natürlich vorher, was das bedeutet), dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist und zeigen ein paar Eigenschaften von Polynomen in $\mathbb{F}_p[X]$.

Quelle: Abschnitt 4.4 in [Smi]. Für den Anfang benötigen wir noch einen Blick in Abschnitt 4.2 von [GG], ab da, wo der letzte Vortrag aufgehört hat. Dass euklidische Ringe faktoriell sind, brauchen wir zum Beweis der zweiten Aussage in Lemma 4.12 in [Smi]. Das findet sich beispielsweise in Abschnitt 2.4 von [Bos].

Vortrag 5: Rechnen in $\mathbb{Z}/n\mathbb{Z}$ (24. 5. 2019)

Als erstes folgern wir den kleinen Satz von Fermat aus dem Satz von Lagrange. Dann wenden wir uns den Rechenoperationen in $\mathbb{Z}/n\mathbb{Z}$ zu: Wir

bestimmen den Aufwand von Addition, Subtraktion, Multiplikation und Inversenbildung (wie in Vortrag 2 durchgeführt) und finden einen effizienten Potenzierungsalgorithmus. Letzteren können wir beispielsweise verwenden, um rechenzeitsparend die Glieder der Fibonaccifolge zu berechnen. Wir zeigen den chinesischen Restsatz einmal als Satz über simultane Kongruenzen und einmal als Struktursatz für $\mathbb{Z}/n\mathbb{Z}$. Letztere Aussage übertragen wir noch auf die multiplikative Gruppe $\mathbb{Z}/n\mathbb{Z}$.

Quelle: Abschnitte 5.1 bis 5.6 (inklusive Aufgabe 5.26) von [BS]. Aus 5.2 soll nur die Aufwandsberechnung, nicht aber noch einmal die Konstruktion der Inversen übernommen werden. Einen Beweis des Satzes von Lagrange findet man zum Beispiel in Abschnitt 1.2 in [Bos], eine Definition der eulerschen φ-Funktion auf Seite 68 in [GG]. Zum chinesischen Restsatz bietet es sich an, ein konkretes Beispiel für ein System von simultanen Konkruenzen vorzurechnen.

Vortrag 6: Quadratische Reste (31. 5. 2019)

Wir definieren m-te Potenzreste und insbesondere quadratische Reste, zeigen das Euler-Kriterium und untersuchen, wieviele quadratische Reste es modulo einer ungeraden Primzahl p gibt. Danach führen wir das Legendre-Symbol ein und zeigen einige seiner Eigenschaften. Höhepunkt des Vortrags ist das Quadratische Reziprozitätsgesetz und sein Beweis.

Quelle: Abschnitte 5.7 und 5.8 in [BS]. Den Beweis des Reziprozitätsgesetzes entnehmen wir [For], 11.2-11.4. Die Anzahl der quadratischen Reste modulo der ungeraden Primzahl p bestimmen wir wie in den Aufgaben 5.15 und 5.16 in [BS] vorgeschlagen und nicht wie in [For]. Wenn noch etwas Zeit ist, kann der Import für den Beweis des Reziprozitätsgesetzes gezeigt werden, dass für p prim das Polynom

$$\phi_p(X) = \sum_{i=0}^{p-1} X^i \in \mathbb{Q}[X]$$

irreduzibel ist, siehe zum Beispiel [For], 5.10-5.11.

Vortrag 7: Carmichaelzahlen und andere Pseudoprimzahlen (7. 6. 2019)

Der kleine Satz von Fermat (s. Vortrag 4) führt uns fast direkt auf den ersten Primzahltest dieses Proseminars, den Fermat'schen Primzahltest. Die Carmichaelzahlen sind nun die zusammengesetzten Zahlen, die dieser Primzahltest nicht als solche erkennt. Wir studieren nun Eigenschaften der Menge dieser „Pseudoprimzahlen“ und wollen sie mit ähnlichen Mengen vergleichen. Dazu verallgemeinern wir das Legendre-Symbol aus dem letzten

Vortrag zum Jacobi-Symbol und führen Euler'sche Pseudoprimzahlen und starke Pseudoprimzahlen ein. Schließlich untersuchen wir, wie diese drei Begriffe zusammenhängen.

Quelle Den Fermat'schen Primzahltest und die Carmichaelzahlen führen wir wie in den Abschnitten 4.3 und 18.2 von [GG] ein. Die Eigenschaften der Carmichaelzahlen und die anderen Pseudoprimzahlbegriffe entnehmen wir Abschnitt 9.3 in [BS]; die Definition des Jacobisymbols ist in Abschnitt 5.9 von [BS] zu finden. Hierbei müssen die Eigenschaften des Jacobisymbols nicht genauer präsentiert werden als in [BS], die Beweise sind sehr analog zu den entsprechenden beim Legendre-Symbol. Satz 5.9.3 sollte genannt aber muss nicht unbedingt bewiesen werden.

Vortrag 8: Probabilistische Primzahltests (14. 6. 2019)

Wir führen eine Reihe neuer Komplexitätsklassen ein (einen ganzer Zoo davon, und wie sie mit $\mathcal{P}$ und $\mathcal{NP}$ zusammenhängen), die von der zufälligen Auswahl einer Variablen abhängen. Wir erklären, was ein Las-Vegas-Algorithmus, ein Atlantic-City-Algorithmus oder ein Monte-Carlo-Algorithmus ist. Anschließend führen wir die Primzahltests von Solovay-Strassen und von Miller-Rabin ein.

Quelle: Die grundlegenden Definitionen finden wir in Abschnitt 3.5 von [BS]; den Rest des Vortrags in Abschnitt 9.4 in [BS]. Abschließend lohnt sich ein Vergleich des Miller-Rabin-Tests mit dem starken Pseudoprimalitätstest aus Abschnitt 18.3 in [GG].

Vortrag 9: Die Riemann'sche Vermutung und der Primzahlsatz (21. 6. 2019)

In diesem Vortrag zeigen wir zunächst eine schwache Version des Primzahlsatzes, die uns später in den Vorträgen über den AKS-Algorithmus genügen wird. Danach skizzieren wir, was heute über dieses Thema bekannt ist. Hierbei wird auch die Riemann'sche Vermutung eingeführt. Wir vergleichen die Aussagen über die Primzahlverteilung mit und ohne Annahme der Riemann'schen Vermutung und führen noch die erweiterte Riemann'sche Vermutung (ERH) ein. Diese nutzen wir schließlich, um verbesserte Primzahltests zu konstruieren.

Quelle: Der Beweis des schwachen Primzahlsatzes findet sich in Abschnitt 4.2 von [Smi]. Der historische Abriss und die Riemann'sche Vermutung mitsamt ihren Auswirkungen auf diesem Gebiet findet sich in Abschnitt 15.3 von [BD]. Zum Vergleich der Verteilungsaussagen ohne und mit Riemann'scher Vermutung ziehen wir 8.2.6 und 8.3.1 in [BS] heran. Schließlich

zitieren wir noch die ERH ([BS], 8.4.4) mit der in Abschnitt 8.4 zuvor eingeführten Notation. Die ERH-basierten Primzahltests entnehmen wir Abschnitt 9.5 von [BS].

Vortrag 10: Der $(n-1)$-Test und Fermatzahlen (28. 6. 2019)

Ausgangspunkt dieses Vortrags ist der Satz von Lucas, der ein weiteres Primalitätskriterium bietet. Diesen beweisen wir und finden mit dem Pepin-Test für Fermatzahlen eine erste Anwendung. Dafür müssen wir natürlich zunächst die Fermatzahlen einführen. Anschließend wollen wir den Primalitätstest aus dem Satz von Lucas noch verfeinern. Das große Problem für die praktische Umsetzung ist nämlich, dass dieser zum Entscheiden der Primalität von n die komplette Primfaktorzerlegung von $n-1$ benötigt. Wir werden zeigen, dass es aber oft genügt, die Primfaktorzerlegung eines hinreichend großen Teilers von $n-1$ zu kennen und werden uns bemühen „hinreichend groß" immer kleiner werden zu lassen. Wenn noch etwas Zeit ist, beenden wir den Vortrag mit den so genannten Lucas-Bäumen.

Quelle: Abschnitt 4.1 in [CP]; die Fermatzahlen werden bereits in Abschnitt 1.3.2 eingeführt.

Vortrag 11: Lineare Codes (5. 7. 2019)

Wir definieren lineare Codes und überlegen uns, wie man mit Methoden der Linearen Algebra Fehler in Datenübertragungen verhindern kann. Es fallen Begriffe wie Hamming-Abstand oder perfekter Code.

Quelle: Das findet man in [JJ], VIII.4. Es lohnt auch ein Blick in VIII.3.

Vortrag 12: Elementare Faktorisierungsmethoden (12. 7. 2019)

Ein dem Primalitätsbeweis ähnliches Problem ist das der Zerlegung einer gegebenen natürlichen Zahl in ihre Primfaktoren. In diesem Vortrag wollen wir zwei Methoden kennen lernen, die besser sind als bloßes Ausprobieren. Zum einen ist das Pollards ϱ-Methode. Um uns einzuarbeiten, zeigen wir zunächst den Geburtstagssatz und Floyds Trick zum Entdecken von Schleifen. Zum anderen ist dies die $(p-1)$-Methode, auch von Pollard. Beides sind probabilistische Tests.

Quelle: Um einen Überblick hinsichtlich des Aufwands moderner Faktorisierungsalgorithmen zu bekommen, lohnt ein Blick in die Einleitung von Kapitel 19 in [GG]. Für die ϱ-Methode orientieren wir uns an Abschnitt 19.4 von [GG], für die $(p-1)$-Methode an Abschnitt 5.4 von [CP]. In beiden Fällen kann das jeweils andere Buch als ergänzende Quelle herangezogen

werden.

Vortrag 13: Polynomidentitäten – Die Idee zu AKS (19. 7. 2019)

In diesem Vortrag zeigen wir zunächst, dass für $n \in \mathbb{N}_{\geq 2}$ und für zu n teilerfremdes $a \in \mathbb{N}$ genau dann

$$(X - a)^n \equiv X^n - a \bmod (n)$$

gilt, wenn n eine Primzahl ist. Aus dieser Aussage lässt sich schnell ein Primalitätstest konstruieren, der jedoch exponentiellen Aufwand verursacht. Um dieses Problem zu umschiffen, verbessern wir die Aussage entscheidend.

Quelle: Die ersten zwei Kapitel aus [Smi] und ebenso die ersten zwei Kapitel aus [AKS]. Die zitierten Aussagen in Kapitel 4 von [Smi] können zu diesem Zeitpunkt alle ohne weiteren Beweis verwendet werden, da sie in früheren Vorträgen gezeigt wurden.

Vortrag 14: Der AKS-Primzahltest (26. 7. 2019)

Wir führen den Primalitätstest von Agrawal, Kayal und Saxena ein und zeigen, dass er polynomielle Laufzeit hat.

Quelle: Kapitel 3 aus [Smi]; der Originalartikel [AKS] ist deutlich schwerer zu lesen. Bei der Laufzeitberechnung müssen wir Kompromisse eingehen: Die Ergebnisse aus Abschnitt 4.5.1 in [Smi] können einfach verwendet werden, die in Abschnitt 4.5.2 wollen wir aber doch zeigen. Bei diesem Vortrag sollte der Vortragende intensiv Rücksprache mit dem Proseminarleiter nehmen.

Literatur

[AKS] Manindra Agrawal, Neeraj Kayal, Nitin Saxena. *PRIMES is in P*. Ann. Math. **160/2** (2004), Seiten 781-793.

[BD] David M. Burton, Heinz Dalkowski. *Handbuch der elementaren Zahlentheorie*. Berliner Studienreihe zur Mathematik, Nr. **12**. Heldermann, 2005.

[Bos] Siegfried Bosch. *Algebra (3. Auflage)*. Springer, 1999.

[BS] Eric Bach, Jeffrey Shallit. *Algorithmic Number Theory – Volume 1: efficient algorithms*. The MIT Press, 1996.

[CP] Richard Crandall, Carl Pomerance. *Prime Numbers – A Computational Perspective*. Springer, 2001.

[For] Otto Forster. *Algorithmische Zahlentheorie*. vieweg, 1996.

[GG] Joachim von zur Gathen, Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

[JJ] Konrad Jacobs, Dieter Jungnickel. *Einführung in die Kombinatorik, 2. völlig neu bearbeitete und erweiterte Auflage*. de Gruyter, 2004.

[Smi] Michiel Smid. *Primality testing in polynomial time*. (online), 2003.