Seminar zur Zahlentheorie

Sommersemester 2011, Mittwoch 10-12 Uhr, T03 R03 D89

Universität Duisburg-Essen
Institut für Experimentelle Mathematik

Prof. Dr. Gabor Wiese
Dr. Panagiotis Tsaknias

Wir begeben uns auf einen Rundgang durch verschiedene Themen der Zahlentheorie, die mit Wissen aus einer der Vorlesungen *Algebra* oder *Anwendungsorientierte Zahlentheorie und Algebra* zugänglich sind. Dabei behandeln wir zunächst die Existenz von unendlich vielen Primzahlen unter bestimmten Kongruenzbedingungen, wenden uns dann der Darstellung von ganzen Zahlen als Summe einer bestimmten Anzahl an Quadratzahlen zu und konzentrieren uns schließlich auf Diophantische Gleichungen; das sind Gleichungen mit ganzzahligen Koeffizienten. Zum Beispiel behandeln wir die einfachsten Fälle der Fermat-Gleichung. Danach betrachten wir die Lösbarkeit bestimmter Diophantischer Gleichungen modulo ganzer Zahlen. Der abschließende beweist Abschätzungen für die Funktion, die Primzahlen zählt. Die ersten zehn Themen sind dem Lehrbuch von Alexander Schmidt *Einführung in die algebraische Zahlentheorie* ([S]) entnommen.

Organisatorisches

- Das Seminar beginnt am Mittwoch, dem 6.4.2011, mit dem ersten Vortrag.
- **Anmeldung:** Bitte melden Sie sich in den Semesterferien an!

  Zur Anmeldung schreiben Sie bitte eine E-Mail (gabor.wiese@uni-due.de) oder rufen an (0201/183-7620). Bei der Anmeldung geben Sie bitte auch gleich einen Wunschvortrag an. Wenn Sie sich nicht sicher sind, welcher Vortrag zu Ihnen passt, dann kommen Sie in die Sprechstunde (in den Semesterferien nach Vereinbarung – also: E-Mail oder Telefon).
- Jeder Vortrag soll detailliert und präzise sein und genügend Beispiele enthalten. Tragen Sie so vor, dass Sie es als Zuhörer selbst verstehen und den Vortrag genießen würden!

  Die Vorträge haben eine Dauer von 90 Minuten. Bei Bedarf können Sie aber auch etwas mehr Zeit erhalten. Denn es ist besser, gut und genau zu erklären, als über die schweren Stellen schnell hinwegzugehen.
- Jeder Vortrag soll spätestens eine Woche vor dem Termin mit Herrn Tsaknias durchgesprochen werden.

Literatur

[S] Alexander Schmidt. *Einführung in die algebraische Zahlentheorie.* Springer-Verlag, 2007. Mit UDE-Kennung elektronisch erhältlich.

Programm

1 Primzahlen mit vorgegebener Restklasse

Bereits Euklid hat zeigen können, dass es unendlich viele Primzahlen gibt. In diesem Vortrag wird diese Aussage wesentlich verschärft: Es wird gezeigt, dass es sogar unendlich viele Primzahlen p gibt, wenn man bestimmte Zusatzbedingungen an die Primzahlen stellt. Zusatzbedingungen, die im Vortrag betrachtet werden, sind: $p \equiv -1 \pmod 3$ ([S], 1.5.1), $p \equiv -1 \pmod 4$ ([S], 1.5.2), $p \equiv 1 \pmod 4$ ([S], 2.3.2), $p \equiv 1 \pmod 3$ ([S], 2.3.4), $p \equiv 1 \pmod 6$ ([S], 2.3, Aufgabe 1), $p \equiv 5 \pmod 6$ ([S], 2.3, Aufgabe 2). Außerdem sollen die Beweise von [S], 2.3.3, 2.3.5 und [S], 2.3.6 gegeben werden. Es bietet sich an, das Gauß'sche Reziprozitätsgesetz zunächst kurz zu wiederholen.

2 Quadratsummen (1. Vortrag)

Eine ganz interessante, klassische Frage lautet, ob eine natürliche Zahl n als Summe einer bestimmten Anzahl an Quadratzahlen dargestellt werden kann. Zum Beispiel ist $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $29 = 2^2 + 5^2$, $21 = 2^2 + 2^2 + 2^2 + 3^2$.

Im Vortrag sollen folgende bemerkenswerte Sätze von Lagrange gezeigt werden:

- *Eine Primzahl $p \neq 2$ ist genau dann Summe von zwei Quadraten, wenn $p \equiv 1 \pmod 4$ gilt.*
- *Jede natürliche Zahl ist Summe von vier Quadraten.*

Im Vortrag soll der gesamte Abschnit 2.4 von [S] behandelt werden mit Ausnahme von 2.4.4, aber unter Einschluss der Aufgabe (wenn die Zeit es erlaubt). Die Hinweise zu den Quaternionen und die Schlussbemerkung dürfen außer Acht gelassen werden.

3 Quadratsummen (2. Vortrag)

Ziel dieses Vortrags ist die folgende Verallgemeinerung eines Satzes des vorherigen Vortrags: *Eine natürliche Zahl ist genau dann Summe von zwei Quadratzahlen, wenn in ihrer Primfaktorzerlegung jede Primzahl kongruent 3 modulo 4 in gerader Vielfachheit vorkommt.*

Um diesen Satz zu beweisen, sollen die Gauß'schen Zahlen wiederholt werden. Dafür sollen die benötigten Fakten aus der Vorlesung *Algebra* oder der Vorlesung *Anwendungsorientierte Zahlentheorie und Algebra* zu Euklidischen und faktoriellen Ringen zusammengestellt werden (präzise und detailliert, aber ohne Beweise) und es soll gezeigt werden, dass $\mathbb{Z}[i]$ ein Euklidischer Ring für die Normfunktion ist, und das Zerlegungsgesetz für Primzahlen im Ring $\mathbb{Z}[i]$ soll bewiesen werden ([S], 4.3.8). Dies füllt den Hauptteil des Vortrags. Der Beweis von [S], Satz 4.4.1, stellt den Höhepunkt und Abschluss der Ausführungen dar.

4 Pythagoräische Tripel

Zunächst sollen alle ganzzahligen Lösungen der Gleichung $X^2 + 1 = Y^3$ bestimmt werden ([S], Satz 4.4.2). Danach geht es um die vollständige Charakterisierung der Pythagoräischen Tripel, also der Zahltripel (a, b, c), die $a^2 + b^2 = c^2$ erfüllen (Beispiel $3^2 + 4^2 = 5^2$).

Davon sollen zwei Beweise angegeben werden: derjenige, der die Arithmetik der Gauß'schen Zahlen benutzt ([S], 4.5.2), und ein geometrischer. Für den geometrischen Beweis soll wie folgt vorgegangen werden: Sei E der Einheitskreis im $\mathbb{R}^2$ und sei $N = (0, 1)$ der 'Nordpol'. Sei nun $P = (\frac{a}{b}, 0)$ ein

Punkt auf der x-Achse mit $\frac{a}{b} \in \mathbb{Q}$. Man berechne die Koordinaten des Schnittpunktes von E mit der Geraden durch N und P. Als Nächstes sei umgekehrt ein Punkt $Q = (x, y) \in E$ mit $x, y \in \mathbb{Q}$ gegeben. Nun berechne man den Schnittpunkt der x-Achse mit der Geraden durch N und Q. Hieraus kann der Satz geschlossen werden.

5 Fermats letzter Satz

Im vorherigen Vortrag wurde gezeigt, dass die Gleichung $X^2 + Y^2 = Z^2$ unendlich viele ganzzahlige Lösungen hat, und diese wurden sogar alle explizit bestimmt. Betrachtet man nicht Quadrate sondern höhere Potenzen, gilt: *Die Gleichung $X^n + Y^n = Z^n$ hat für $n \geq 3$ keine Lösungen in positiven ganzen Zahlen.* Dieses wurde von Fermat behauptet, aber erst 1994 von Wiles bewiesen.

Im Vortrag sollen der Fall $n = 4$ und der Satz von Sophie Germain bewiesen werden ([S], Kapitel 7).

6 Diophantische Gleichungen modulo p (1. Vortrag)

Eine häufig wesentlich einfachere Frage als die nach ganzzahligen Lösungen von Gleichungen ist die nach Lösungen modulo p für eine Primzahl p. In diesem Vortrag soll hauptsächlich der Satz von Chevalley-Warning bewiesen werden, der eine hinreichende Bedingung für die Existenz von Lösungen modulo p angibt ([S], 3.3.1 und 3.3.2). Dieser soll durch Beispiele illustriert werden. Im Vortrag soll aber zunächst allgemein über reelle Hindernisse und Hindernisse modulo m ([S], 3.1) berichtet werden (jeweils mit mindestens einem Beispiel).

7 Dirichlet-Charaktere

Es sollen Dirichlet-Charaktere wie im Abschnitt 8.1 von [S] behandelt werden.

8 Gauß- und Jacobi-Summen

Es sollen Gauß- und Jacobi-Summen wie im Abschnitt 8.2 von [S] behandelt werden.

9 Diophantische Gleichungen modulo p (2. Vortrag)

Dieser Vortrag benutzt die Resultate aus dem vorherigen, um zu zeigen, dass die Gleichung $aX^4 + bX^4 = c$ modulo jeder Primzahl $p \equiv 1 \mod 4$, $p > 41$, eine Lösung hat ([S], 8.3). Außerdem soll begonnen werden, die Gleichung $X^4 - 17 = 2Y^2$ zu untersuchen. Es sollen die Lemmata [S], 3.5.2, 3.5.3, 3.5.4 und 3.5.5 gezeigt werden.

10 Diophantische Gleichungen modulo p (3. Vortrag)

Unter bestimmten Voraussetzungen kann man aus der Lösung einer Gleichung modulo p^n (mit p Primzahl) schließen, dass es eine Lösung modulo p^{n+1} gibt. Der entsprechende Satz ist [S], 3.4.1, und soll bewiesen werden. Er soll angewendet werden, um zu zeigen, dass die bereits im vorherigen Vortrag behandelte Gleichung $X^4 - 17 = 2Y^2$ eine Lösung modulo jeder natürlichen Zahl hat. Allerdings hat diese Gleichung keine Lösung in $\mathbb{Q}$, wie abschließend bewiesen werden soll ([S], 3.5.11).

11 Tschebyschows Satz

Sei $\pi(x)$, für $x \in \mathbb{R}$, die Anzahl der Primzahlen $p \leq x$. Tschebyschow hat 1850 bewiesen, dass es bestimmte explizite Zahlen c und C gibt, so dass folgende Abschätzung gilt:

$$c\frac{x}{\log x} \leq \pi(x) \leq C\frac{x}{\log x}.$$

Das Ziel dieses Vortrags ist, diesen Satz zu beweisen. Der/die Vortragende soll dabei u.a. die folgenden Funktionen/Notationen einführen und benutzen: Von Mangoldts Funktion $\Lambda(n)$ und Tschebyschows Funktionen $\theta(x)$ und $\psi(x)$.

Der/die Vortragende sollte auch Bertrands Postulat beweisen: Für jedes $n > 1$ existiert mindestens eine Primzahl zwischen n und $2n$. Die Methoden für den Beweis sind den Methoden für den Beweis von Tschebyschows Satz sehr ähnlich.

Verweise für diese Materie sind z.B. Sektionen 22.1 bis 22.4 in Hardy-Wright (siehe Kapitel 1 für die Notationen, die in Kapitel 22 benutzt werden) und Sektionen 1.6 und 2.4 in Jameson (Satz 2.3.4 für die Definition von $\Lambda(n)$).

Literatur für diesen Vortrag:

G. H. Hardy und E. M. Wright. *An introduction to the theory of numbers (4th edition).* Oxford University Press, 1975.

G. J. O. Jameson. *The Prime Number Theorem.* LMS Student Texts **53**, Cambridge University Press, 2003.