Blockseminar Algebra/Zahlentheorie

Themen

Jun. Prof. Dr. Jeroen Sijsling
Jeroen Hanselman
Institut für Reine Mathematik
Wintersemester 2018-2019
✉ *jeroen.sijsling@uni-ulm.de*

Bitte wählen Sie fünf von diesen Themen, stufen Sie sie ein, und schicke Sie Ihre Präferenzen an mich. Die Verteilung unter den Teilnehmern findet dann statt mithilfe eines Algorithmus.

In allen Vorträgen soll eine aktive Teilnahme aller Studierende stimuliert werden! Versuchen Sie, schöne interaktive Beispiele zu finden und zu verwenden.

Themen

1. Kettenbrüche

Kettenbrüche sind Ausdrücke der Form

$$2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\cdots}}}}}}}}$$

Jeder gewönhliche Bruchzahl hat auch eine Beschreibung als Kettenbruch. Interessanter ist aber, dass auch jeder reelle Zahl eine unendliche Kettenbruchentwicklung hat. So ist die Entwicklung oben der Anfang der unendlichen Kettenbruchentwicklung von e. Deren endlichen Teilentwicklungen liefern die besten Approximationen von reellen Zahlen durch Bruchzahlen: So bekommen wir zum Beispiel $\pi \approx \frac{22}{7}$ und, noch besser,

$$\pi \approx \frac{355}{113}.$$

Weiter kann man die Frage stellen, welche Zahlen eine periodische Kettenbruchentwicklung haben: Dies sind genau die Quadratzahlen.

Quelle: [3, §12].

2. Die Pellsche Gleichung

Sei N eine ganze Zahl, die kein Quadrat ist. Dann wird die Gleichung

$$x^2 - Ny^2 = 1$$

für $x, y \in \mathbb{Z}$ auch die *Pellsche Gleichung* genannt. Diese Gleichungen waren schon den alten Griechen und Indern bekannt, und teilweise Lösungsmethoden wurden schon von ihnen beschrieben. Wir studieren diese Methoden und geben Anwendungen, wie die Bestimmung aller Quadraten die auch Drieeckszahlen sind. Eine letzte interessante Frage ist: *Warum* können wir diese Fragen lösen? Hier spielen abstraktere algebraische Betrachtungen und sogenannte *Einheitengruppen* eine Rolle.

Quelle: [3, §13].

3. Summen von Quadraten

Sei n eine positive und quadratfreie ganze Zahl. Wann ist n eine Summe zweier Quadraten, dass heisst, wann gilt

$$n = x^2 + y^2$$

für irgendwelche $x, y \in \mathbb{Z}$? Unerwarteterweise ist die Antwort ganz einfach: dies ist der Fall genau dann, wenn alle Primfaktoren p von n die Eigenschaft haben, dass $p \equiv 1 \pmod 4$. Der Beweis dieser Aussage verwendet die arithmetische Struktur der *Gausschen ganzen Zahlen*

$$\mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}\}\,.$$

Genau wie für "normale" ganze Zahlen können wir zwei solche Zahlen mit Rest durcheinander teilen. Diese wesentliche algebraische Eigenschaft erlaubt es, die oben erwähnte Aussage zu zeigen. Weiter gibt es einen zweiten Satz von Lagrange, welcher zeigt, dass alle positive Zahlen Summen vierer Quadrate sind.

Quelle: [3, §13].

4. Quadratische Reziprozität

Seien p und q zwei verschiedene Primzahle. Wir definieren das *Legendre-Symbol* wie folgt:

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{wenn } p \mid n \\ 1 & \text{wenn } n \text{ ein Quadrat mod } p \\ -1 & \text{wenn } n \text{ kein Quadrat mod } p \end{cases}$$

Quadratische Reziprozität zeigt, wie die Werte $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$ zusammenhängen. Dieser Satz hat unglaublich viele Beweise, auch ein sehr elementaren, welchen Sie zuerst zeigen können. Eine mehr aufschlussreiche Beweis ist jener, der zuerst zeigt, dass $\left(\frac{p}{q}\right)$ nur der Kongruenzklasse von q modulo $4p$ abhängig ist. Dieser Beweis verwendet abstraktere algebraische Strukturen, die *Zahlkörper* genannt werden. Hier reicht es, die Idee zu skizzieren.

Quelle: [3, §11].

5. Primzahlzerlegung

Sei n eine große Zahl, die wir als Produkt von Primzahlen schreiben wollen. Wie zerlegen wir n? Es gibt jetzt viele kräftige Methoden zu diesem Zweck. Wir betrachten aber einige klassische Verfahren. Die $p-1$-*Methode* von Pollard liefert alle Primfaktoren p von n mit der Eigenschaft, dass $p-1$

ein Produkt von vielen kleinen Zahlen ist. Solche Zahlen $p-1$ heissen *glatt*. Diese Methode reicht schon für die Zerlegung von vielen Zahlen.

In der $p-1$-Methode spielt die Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ eine wesentliche Rolle. Die Methode funktioniert aber auch für allgemeinere Gruppen, deren Ordnung $p+k$ sich wenig von p unterschiedet. Dies liefert auch eine Chance, um diejenigen Primfaktoren p zu bestimmen, mit der Eigenschaft, dass $p+k$ glatt ist. Die genaue Beschreibung dieser Gruppen, die von *elliptischen Kurven* kommen, würde zu weit führen. Jedoch können Sie im Vortrag eine abstrakte Betrachtung der fundamentalen Idee geben.

Quelle: [3, §9].

6. Primzahltests

Wie können wir eine große Primzahl finden? Eine Antwort ist: Wir konstruieren eine beliebige große Zahl p, und versuchen es zu zerlegen mit den Methoden des letzten Vortrags. Dies ist aber keine gute Idee, weil das Bestimmen von Zerlegungen noch immer sehr viel Aufwand kostet. Jedoch gibt es allgemeine Methoden, die bestimmen, ob eine Zahl Prim ist oder nicht. Dies ist deshalb der Fall, weil wenn die Zahl nicht eine Primzahl ist, die Methode ihre Zerlegung nicht bestimmen.

Ein allgemeines Verfahren zu diesem Zweck ist die Methode von Lukas. Sie setzt voraus, dass wir $p-1$ zerlegen können. Wenn das der Fall ist, so wendet sie den kleinen Fermatschen Satz an, um ein Kriterium zu lieferen, das bestimmt, ob p eine Primzahl ist oder nicht.

Aber was, wenn wir zudem akzeptieren, dass unsere Primzahl p von einer bestimmten Form ist? Dies kann die Arbeit beträchtlich erleichtern! Proth hat einen Primzahltest entwickelt für Zahlen der Form $k2^n+1$ mit $k<2^n$ ungerade. Dies erlaubt die Konstruktion von recht großen Primzahlen: Die kleinste bekannste Primzahl, die keine Mersenne-Zahl ist, ist der beschriebenen Form.

Quelle: [3, §9].

7. RSA-Verfahren

Das RSA-Verfahren haben wir schon in der Vorlesung *Elementare Zahlentheorie* gesehen, also brauchen wir nur eine sehr kurze Wiederholung. Interessanter sind Angriffe auf das Verfahren.

Stellen Sie sich zum Beispiel vor, dass ich Ihr Gegner bin und einen affinen Schlüssel verwende. Vielleicht wissen Sie, dass ich meine Nachrichten immer mit "Viele Grüße, Jeroen Sijsling" unterschreibe. Dann können Sie meinen Schlüssel finden und meine Nachrichten lesen. Dies ist ein Beispiel der *Known-Plaintext-Angriff*, die auch im zweiten Weltkrieg beim Entschlüsselen des Enigma-Systems verwendet wurde. Andere Methoden, wie der *Chosen-Ciphertext-Angriff*, existieren auch. Und natürlich gibt es im RSA-Verfahren Verteidigungen gegen sie.

Es könnte in diesem Vortrag auch interessant sein, die Installation und Verwendung vom PGP-Verfahren zu demonstrieren. Dies ist also einen Vortrag für mehr Informatikorientierte Studierende.

Quelle: [1, §9].

8. Geheimnisteilung

Geheimnisteilung wird ermöglicht durch das *Diffie–Hellman-Verfahren*, ein Verfahren, dass wir auch schon in der Vorlesung *Elementare Zahlentheorie* gesehen haben. Es ist basiert auf die Schwierigkeit,

diskrete Logarithmen in einem allgemeinen zyklischen Gruppe G zu finden.

Es existieren aber Methoden, um doch solche Logarithmen zu berechnen. Die erste ist basiert auf dem *Babystep-Giantstep-Algorithmus*, eine Idee, die in vielen Bereichen Anwendungen gefunden hat. Sie funktioniert für *alle* zyklischen Gruppen G. Eine zweite Methode ist die von Pollig–Hellman: Sie funktioniert fur die Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$, wenn $p-1$ eine glatte Zahl ist. Dies zeigt, wie wichtig die Wahl der Gruppe G ist, um sicher zu stellen, dass das Diffie–Hellman-Verfahren nicht geknackt werden kann. Auch hier spielen elliptische Kurven wieder eine Rolle...

Quelle: [1, §3].

9. Digitale Unterschiften

Mit RSA ist es möglich, eine Nachricht zu unterschreiben. Nur *Sie* können die Unterschrift herstellen, aber *alle* können sie verifizieren. Hiermit sind Empfänger also sicher, dass eine Nachricht von Ihnen kommt.

Auch auf diesem Verfahren gibt es Angriffe. Um diese zu vermeiden, werden *Hashfunktionen* verwendet. Diese Funktionen spielen auch eine Rolle im *TLS-Verfahren*. Dieses spielt eine Rolle in ihrem Browser, wenn es eine HTTPS-Seite besucht. Mehr information finden sie auf

`https://en.wikipedia.org/wiki/Transport_Layer_Security`

Auch dieser Vortrag ist interessant für mehr Informatikorientierte Studierende: Sie können eine mehr detaillierte Beschreibung dieses Verfahrens geben.

Quelle: [1, §6].

10. Münzwürfe

Wir wollen einen ehrlichen Münzwurf machen. Was aber, wenn Sie mich nicht vertrauen? Vielleicht habe ich die Münze manipuliert, oder vielleicht sind wir weit von einander, reden wir über Skype oder, wenn wir gewissenshaft sind, über Ring (`https://ring.cx/`) und können Sie nicht sehen, ob ich den Wurf ehrlich mache. Was dann?

Hier existiert ein Verfahren, wo wir beide sicher sein können. Es heisst das *Blum-Münzwurfprotokoll*, und basiert sich auf die Schwierigkeit, die Lösungen von

$$x^2 \equiv a \pmod{pq}$$

zu bestimmen, wenn p und q große unbekannte Primzahlen sind. Ihre Aufgabe ist die Beschreibung und Durchführung dieses Verfahrens.

Quelle: [1, §7].

11. Kenntnisfreie Protokolle

Stellen wir uns vor, Sie haben ein Kennwort. Normalerweise geben Sie das Kennwort ein, um zu bestätigen, dass Sie es sind. Vielleicht sind Sie aber nicht ganz sicher, dass diejenige Person, an die Sie normalerweise dieses Kennwort geben würden, auch vertrauenswürdig ist. Ist es vielleicht möglich, jemand davon zu überzeugen, dass ihr Kennwort stimmt, ohne es explizit zu geben, und ohne irgendwelche Information über dieses Kennwort auszutauschen?

Dies scheint wirklich unmöglich. Aber jedoch existieren Protokolle, die es ermöglichen. Sie heissen *Kenntnisfreie Protokolle* oder *Zero-Knowledge Protokolle*, und sind basiert auf die oben erwähnten Schwierigkeit, Quadratwurzeln modulo pq zu bestimmen, wenn p und q nicht bekannt sind. Auch eine andere Variante existiert: Sie verwendet das diskrete Logarithmus-Verfahren. Die Beschreibung dieser Verfahren ist das Thema dieses Vortrags.

Quelle: [1, §7], [2].

Literatur

[1] Irene Bouw, Vorlesungsskript *Kryptologie*.

[2] Tom Berson, Louis Guillou, and Jean-Jacques Quisquater, *How to Explain Zero-Knowledge Protocols to Your Children*.

[3] Kenneth Rosen, *Elementary Number Theory and its applications*.