Algebra und Zahlentheorie

Organisatorisches und ein bisschen Motivation

Martin Hofer

13. Oktober 2015

Allgemeines

Alle relevanten Informationen zum Übungsbetrieb der Veranstaltungen Algebra und Zahlentheorie finden Sie auf:

`www.mathematik.uni-muenchen.de/~hofer/algws15`

Angebotene Tutorien:

Wochentag	Uhrzeit	Tutorin/Tutor
Montag	08-10 Uhr	Pascal Stucky
Montag	12-14 Uhr	Hannah Schrenk
Dienstag	08-10 Uhr	Pascal Stucky
Donnerstag	10-12 Uhr	Hannah Schrenk
Donnerstag	14-16 Uhr	Dominik Bullach
Freitag	10-12 Uhr	Chris Geishauser

Es gibt in jedem Tutorium 30 Plätze; bitte nur ein Tutorium besuchen.

Änderungen zu den Vorjahren

Änderungen zu den Vorjahren

i) Gemeinsamer Übungsbetrieb für beide Veranstaltungen, d.h., gemeinsame Tutorien und Zentralübung, gemeinsames Übungsblatt

Änderungen zu den Vorjahren

i) Gemeinsamer Übungsbetrieb für beide Veranstaltungen, d.h., gemeinsame Tutorien und Zentralübung, gemeinsames Übungsblatt

ii) *Aber:* Bonusregelungen, Klausuren und Vorlesungsprotokolle getrennt; auf gemeinsamen Übungsblatt sind die Beispiele jeweils einer der beiden Veranstaltung zugeordnet

Änderungen zu den Vorjahren

i) Gemeinsamer Übungsbetrieb für beide Veranstaltungen, d.h., gemeinsame Tutorien und Zentralübung, gemeinsames Übungsblatt

ii) *Aber:* Bonusregelungen, Klausuren und Vorlesungsprotokolle getrennt; auf gemeinsamen Übungsblatt sind die Beispiele jeweils einer der beiden Veranstaltung zugeordnet

iii) Es wird keine Musterlösungen zu den Aufgaben geben; wir besprechen die Übungsblattaufgaben in der Zentralübung.

Änderungen zu den Vorjahren

i) Gemeinsamer Übungsbetrieb für beide Veranstaltungen, d.h., gemeinsame Tutorien und Zentralübung, gemeinsames Übungsblatt

ii) *Aber:* Bonusregelungen, Klausuren und Vorlesungsprotokolle getrennt; auf gemeinsamen Übungsblatt sind die Beispiele jeweils einer der beiden Veranstaltung zugeordnet

iii) Es wird keine Musterlösungen zu den Aufgaben geben; wir besprechen die Übungsblattaufgaben in der Zentralübung.

iv) Es wird keine Tutoriumsblätter geben; Aufgaben werden in Tutorien ausgegeben und besprochen.

Abgabe/Ausgabe Übungsblätter - Bonusregelung

Abgabe/Ausgabe Übungsblätter - Bonusregelung

i) Ausgabe der Übungsblätter Mittwoch Nachmittag, erstmalig morgen 14. Oktober

Abgabe/Ausgabe Übungsblätter - Bonusregelung

i) Ausgabe der Übungsblätter Mittwoch Nachmittag, erstmalig morgen 14. Oktober

ii) Bearbeitungszeit fast eine Woche

Abgabe/Ausgabe Übungsblätter - Bonusregelung

i) Ausgabe der Übungsblätter Mittwoch Nachmittag, erstmalig morgen 14. Oktober

ii) Bearbeitungszeit fast eine Woche

iii) Abgabe Mittwoch 10 Uhr in Übungskasten im 1. Stock

Abgabe/Ausgabe Übungsblätter - Bonusregelung

i) Ausgabe der Übungsblätter Mittwoch Nachmittag, erstmalig morgen 14. Oktober

ii) Bearbeitungszeit fast eine Woche

iii) Abgabe Mittwoch 10 Uhr in Übungskasten im 1. Stock

iv) Mit 50 Prozent der Übungspunkte der Aufgaben die der Veranstaltung zugeordnet sind, verbessert sich die Note einer bestandenen Klausur um eine Notenstufe.

Abgabe/Ausgabe Übungsblätter - Bonusregelung

i) Ausgabe der Übungsblätter Mittwoch Nachmittag, erstmalig morgen 14. Oktober

ii) Bearbeitungszeit fast eine Woche

iii) Abgabe Mittwoch 10 Uhr in Übungskasten im 1. Stock

iv) Mit 50 Prozent der Übungspunkte der Aufgaben die der Veranstaltung zugeordnet sind, verbessert sich die Note einer bestandenen Klausur um eine Notenstufe.

Fragen

Gibt es noch Fragen zum Übungsbetrieb?

MAGMA-Kurs

MAGMA-Kurs

Termin

Donnerstag, 14-16 Uhr (direkt an der Algebravorlesung) im CIP-Raum BU136.

MAGMA-Kurs

Termin

Donnerstag, 14-16 Uhr (direkt an der Algebravorlesung) im CIP-Raum BU136.

Anmeldung

Über den Lecture-Assistant, begrenzte Teilnehmerzahl: 30; Anmeldung starte heute (13.Oktober) Nachmittag

Warum Algebra und Zahlentheorie?

Warum Algebra und Zahlentheorie?

i) Viele Konzepte, Definitionen und Theoreme der Algebra und Zahlentheorie aus 'fast alltäglichen' Fragestellungen entstanden.

Warum Algebra und Zahlentheorie?

i) Viele Konzepte, Definitionen und Theoreme der Algebra und Zahlentheorie aus 'fast alltäglichen' Fragestellungen entstanden.

ii) In den letzten 40 Jahren wurden einige Anwendungen außerhalb der reinen Mathematik gefunden:
zB Kryptographie und Kryptoanalyse.

Warum Algebra und Zahlentheorie?

i) Viele Konzepte, Definitionen und Theoreme der Algebra und Zahlentheorie aus 'fast alltäglichen' Fragestellungen entstanden.

ii) In den letzten 40 Jahren wurden einige Anwendungen außerhalb der reinen Mathematik gefunden:
zB Kryptographie und Kryptoanalyse.

iii) Grundvoraussetzung für viele andere Teilgebiete der Mathematik und theoretischen Physik (zB Gruppentheorie)

Warum Algebra und Zahlentheorie?

i) Viele Konzepte, Definitionen und Theoreme der Algebra und Zahlentheorie aus 'fast alltäglichen' Fragestellungen entstanden.

ii) In den letzten 40 Jahren wurden einige Anwendungen außerhalb der reinen Mathematik gefunden:
zB Kryptographie und Kryptoanalyse.

iii) Grundvoraussetzung für viele andere Teilgebiete der Mathematik und theoretischen Physik (zB Gruppentheorie)

iv) Essentieller Bestandteil der Lehrerausbildung (Staatsexamen Algebra).

Warum Algebra und Zahlentheorie?

i) Viele Konzepte, Definitionen und Theoreme der Algebra und Zahlentheorie aus 'fast alltäglichen' Fragestellungen entstanden.

ii) In den letzten 40 Jahren wurden einige Anwendungen außerhalb der reinen Mathematik gefunden:
zB Kryptographie und Kryptoanalyse.

iii) Grundvoraussetzung für viele andere Teilgebiete der Mathematik und theoretischen Physik (zB Gruppentheorie)

iv) Essentieller Bestandteil der Lehrerausbildung (Staatsexamen Algebra).

Was ich heute verdeutlichen will

Vieles was war aktuell in der Algebra und Zahlentheorie lernen, ist auf Fragestellungen der elementaren Zahlentheorie zurückzuführen.

Fragen zu Primzahlen

Fragen zu Primzahlen

Frage

Wie viele Primzahlen gibt es?

Fragen zu Primzahlen

Frage

Wie viele Primzahlen gibt es?

Theorem (Euklid)

Es gibt unendlich viele Primzahlen.

Fragen zu Primzahlen

Frage

Wie viele Primzahlen gibt es?

Theorem (Euklid)

Es gibt unendlich viele Primzahlen.

Proof.

Für eine beliebige endliche Menge $\{p_1, \ldots, p_r\}$ von Primzahlen sei $n := p_1 p_2 \cdots p_r + 1$ und p ein Primteiler von n. Wir sehen, dass p von allen p_i verschieden ist, da sonst p sowohl die Zahl n als auch das Produkt $p_1 p_2 \cdots p_r$ teilen würde, somit auch die 1, was nicht sein kann. Eine endliche Menge kann also niemals die Menge aller Primzahlen sein. □

Frage

Wie sind die Primzahlen verteilt?

Frage

Wie sind die Primzahlen verteilt?

Definition

Wir definieren die *Primzahlfunktion* $\pi(x)$ durch

$$\begin{aligned} \pi : \mathbb{R}^+ &\to \mathbb{N}_0, \\ x &\mapsto \#\{p \text{ Primzahl} \mid p \leq x\}. \end{aligned}$$

Frage

Wie sind die Primzahlen verteilt?

Definition

Wir definieren die *Primzahlfunktion* $\pi(x)$ durch

$$\begin{aligned} \pi : \mathbb{R}^+ &\to \mathbb{N}_0, \\ x &\mapsto \#\{p \text{ Primzahl} \mid p \leq x\}. \end{aligned}$$

Theorem

Die oben definierte Primzahlfunktion hat folgendes asymptotisches Verhalten:

$$\lim_{x \to \infty} \pi(x) \left(\frac{x}{\ln(x)} \right)^{-1} = 1$$

Zum Beweis des Primzahlsatzes

Riemann: Verbindung zw. der Verteilung der Primzahlen und den Eigenschaften der Riemann'schen Zetfunktion $\zeta(s)$:
Primzahlsatz äquivalent dazu ist, dass $\zeta(s)$ keine Nullstellen mit Realteil 1 hat.
Hadamard und de Vallee-Poussin haben 1896 beweisen das unter Benutzung funktionentheoretischer Methoden bewiesen.
'Elementare' Beweise wurden erst 1949 von Atle Selberg und Paul Erdös gefunden.

Zum Beweis des Primzahlsatzes

Riemann: Verbindung zw. der Verteilung der Primzahlen und den Eigenschaften der Riemann'schen Zetfunktion $\zeta(s)$:
Primzahlsatz äquivalent dazu ist, dass $\zeta(s)$ keine Nullstellen mit Realteil 1 hat.
Hadamard und de Vallee-Poussin haben 1896 beweisen das unter Benutzung funktionentheoretischer Methoden bewiesen.
'Elementare' Beweise wurden erst 1949 von Atle Selberg und Paul Erdös gefunden.

Moral I: In der Zahlentheorie ist es oft hilfreich Hilfsmittel aus anderen mathematischen Teildisziplinen zu benutzen.

Zum Beweis des Primzahlsatzes

Riemann: Verbindung zw. der Verteilung der Primzahlen und den Eigenschaften der Riemann'schen Zetfunktion $\zeta(s)$:
Primzahlsatz äquivalent dazu ist, dass $\zeta(s)$ keine Nullstellen mit Realteil 1 hat.
Hadamard und de Vallee-Poussin haben 1896 beweisen das unter Benutzung funktionentheoretischer Methoden bewiesen.
'Elementare' Beweise wurden erst 1949 von Atle Selberg und Paul Erdös gefunden.

Moral I: In der Zahlentheorie ist es oft hilfreich Hilfsmittel aus anderen mathematischen Teildisziplinen zu benutzen.
Moral II: Wer sich den 'elementaren Beweis' ansieht wird feststellen: elementar $\neq$ einfach.

Frage

Ist eine gegebene Zahl eine Primzahl oder zusammengesetzt?

Frage

Ist eine gegebene Zahl eine Primzahl oder zusammengesetzt?

i) Man löst solche Probleme durch Angabe von Algorithmen deren Laufzeit möglichst langsam wächst im Vergleich zur Eingabelänge des Inputs des Algorithmus.

Frage

Ist eine gegebene Zahl eine Primzahl oder zusammengesetzt?

i) Man löst solche Probleme durch Angabe von Algorithmen deren Laufzeit möglichst langsam wächst im Vergleich zur Eingabelänge des Inputs des Algorithmus.
ii) Man kann Algorithmen nach Laufzeit unterscheiden in polynomielle und exponentielle Algorithmen.

Frage

Ist eine gegebene Zahl eine Primzahl oder zusammengesetzt?

i) Man löst solche Probleme durch Angabe von Algorithmen deren Laufzeit möglichst langsam wächst im Vergleich zur Eingabelänge des Inputs des Algorithmus.
ii) Man kann Algorithmen nach Laufzeit unterscheiden in polynomielle und exponentielle Algorithmen.
iii) Man kann Algorithmen in deterministische oder probabilistische Algorithmen, d.h., je nach dem ob ein Ergebnis mit hoher Wahrscheinlichkeit richtig ist oder sicher richtig ist.

Frage

Ist eine gegebene Zahl eine Primzahl oder zusammengesetzt?

i) Man löst solche Probleme durch Angabe von Algorithmen deren Laufzeit möglichst langsam wächst im Vergleich zur Eingabelänge des Inputs des Algorithmus.
ii) Man kann Algorithmen nach Laufzeit unterscheiden in polynomielle und exponentielle Algorithmen.
iii) Man kann Algorithmen in deterministische oder probabilistische Algorithmen, d.h., je nach dem ob ein Ergebnis mit hoher Wahrscheinlichkeit richtig ist oder sicher richtig ist.
iv) Es gibt eine deterministischen polynomiellen Algorithmus der entscheidet, ob eine Zahl eine Primzahl ist.

Frage

Ist eine gegebene Zahl eine Primzahl oder zusammengesetzt?

i) Man löst solche Probleme durch Angabe von Algorithmen deren Laufzeit möglichst langsam wächst im Vergleich zur Eingabelänge des Inputs des Algorithmus.
ii) Man kann Algorithmen nach Laufzeit unterscheiden in polynomielle und exponentielle Algorithmen.
iii) Man kann Algorithmen in deterministische oder probabilistische Algorithmen, d.h., je nach dem ob ein Ergebnis mit hoher Wahrscheinlichkeit richtig ist oder sicher richtig ist.
iv) Es gibt eine deterministischen polynomiellen Algorithmus der entscheidet, ob eine Zahl eine Primzahl ist.
v) Dieser wurde 2002 von Agrawal, Kayal und Saxena gefunden unter Verwendung einer Verallgemeinerung des kleinen Satz von Fermat, den wir in der Gruppentheorie beweisen werden.

Frage

Wie kann man möglichst effizient Zahlen faktorisieren oder wie sicher sind gängige Verschlüsselungsverfahren?

Frage

Wie kann man möglichst effizient Zahlen faktorisieren oder wie sicher sind gängige Verschlüsselungsverfahren?

i) Faktorisierung, d.h. finde p oder q für $n = pq$ ist zeitaufwändig; bei 'naiven Algorithmen' wächst die Laufzeit exponentiell in Bezug auf die Eingabelänge.

Frage

Wie kann man möglichst effizient Zahlen faktorisieren oder wie sicher sind gängige Verschlüsselungsverfahren?

i) Faktorisierung, d.h. finde p oder q für $n = pq$ ist zeitaufwändig; bei 'naiven Algorithmen' wächst die Laufzeit exponentiell in Bezug auf die Eingabelänge.

ii) Beispiel einer 'one-way'-Funktion, d.h. leicht zu berechnen (Multiplikation), schwierig zu invertieren (Faktorisierung).

Frage

Wie kann man möglichst effizient Zahlen faktorisieren oder wie sicher sind gängige Verschlüsselungsverfahren?

i) Faktorisierung, d.h. finde p oder q für $n = pq$ ist zeitaufwändig; bei 'naiven Algorithmen' wächst die Laufzeit exponentiell in Bezug auf die Eingabelänge.
ii) Beispiel einer 'one-way'-Funktion, d.h. leicht zu berechnen (Multiplikation), schwierig zu invertieren (Faktorisierung).
iii) Die Sicherheit von gängigen Verschlüsselungsverfahren (RSA) beruht also darauf, dass die Komplexität der Berechnung der Faktorisierung höher ist, als die der Multiplikation.

Frage

Wie kann man möglichst effizient Zahlen faktorisieren oder wie sicher sind gängige Verschlüsselungsverfahren?

i) Faktorisierung, d.h. finde p oder q für $n = pq$ ist zeitaufwändig; bei 'naiven Algorithmen' wächst die Laufzeit exponentiell in Bezug auf die Eingabelänge.
ii) Beispiel einer 'one-way'-Funktion, d.h. leicht zu berechnen (Multiplikation), schwierig zu invertieren (Faktorisierung).
iii) Die Sicherheit von gängigen Verschlüsselungsverfahren (RSA) beruht also darauf, dass die Komplexität der Berechnung der Faktorisierung höher ist, als die der Multiplikation.
iv) Es gibt keine klassischen Algorithmen, die in polynomieller Zeit eine Zahl faktorisieren.

Frage

Wie kann man möglichst effizient Zahlen faktorisieren oder wie sicher sind gängige Verschlüsselungsverfahren?

i) Faktorisierung, d.h. finde p oder q für $n = pq$ ist zeitaufwändig; bei 'naiven Algorithmen' wächst die Laufzeit exponentiell in Bezug auf die Eingabelänge.
ii) Beispiel einer 'one-way'-Funktion, d.h. leicht zu berechnen (Multiplikation), schwierig zu invertieren (Faktorisierung).
iii) Die Sicherheit von gängigen Verschlüsselungsverfahren (RSA) beruht also darauf, dass die Komplexität der Berechnung der Faktorisierung höher ist, als die der Multiplikation.
iv) Es gibt keine klassischen Algorithmen, die in polynomieller Zeit eine Zahl faktorisieren.
v) Es gibt aber Quantenalgorithmen, die in polynomieller Zeit eine Zahl faktorisieren. Problem: Bisher nur theoretisches Konstrukt, Umsetzung wird noch einige Jahrzehnte dauern.

Fragen zu algebraischen Gleichungen

Fragen zu algebraischen Gleichungen

Frage

Wie viele Lösungen hat eine algebraische Gleichung (polynomiale Gleichung) n-ten Grades?

Fragen zu algebraischen Gleichungen

Frage

Wie viele Lösungen hat eine algebraische Gleichung (polynomiale Gleichung) n-ten Grades?

Es kommt natürlich auf den zugrundeliegenden Körper an. Für die komplexen Zahlen haben wir:

Fragen zu algebraischen Gleichungen

Frage

Wie viele Lösungen hat eine algebraische Gleichung (polynomiale Gleichung) n-ten Grades?

Es kommt natürlich auf den zugrundeliegenden Körper an. Für die komplexen Zahlen haben wir:

Theorem (Fundamentalsatz der Algebra - Gauss)

Jedes nichtkonstante Polynom mit komplexen Koeffizienten besitzt mindestens eine komplexe Nullstelle.

Fragen zu algebraischen Gleichungen

Frage

Wie viele Lösungen hat eine algebraische Gleichung (polynomiale Gleichung) n-ten Grades?

Es kommt natürlich auf den zugrundeliegenden Körper an. Für die komplexen Zahlen haben wir:

Theorem (Fundamentalsatz der Algebra - Gauss)

Jedes nichtkonstante Polynom mit komplexen Koeffizienten besitzt mindestens eine komplexe Nullstelle.

Bemerkung

Fragen zu algebraischen Gleichungen

Frage

Wie viele Lösungen hat eine algebraische Gleichung (polynomiale Gleichung) n-ten Grades?

Es kommt natürlich auf den zugrundeliegenden Körper an. Für die komplexen Zahlen haben wir:

Theorem (Fundamentalsatz der Algebra - Gauss)

Jedes nichtkonstante Polynom mit komplexen Koeffizienten besitzt mindestens eine komplexe Nullstelle.

Bemerkung

Man benötigt Methoden aus der Analysis um diesen Satz zu beweisen.

Fragen zu algebraischen Gleichungen

Frage

Wie viele Lösungen hat eine algebraische Gleichung (polynomiale Gleichung) n-ten Grades?

Es kommt natürlich auf den zugrundeliegenden Körper an. Für die komplexen Zahlen haben wir:

Theorem (Fundamentalsatz der Algebra - Gauss)

Jedes nichtkonstante Polynom mit komplexen Koeffizienten besitzt mindestens eine komplexe Nullstelle.

Bemerkung

Gibt natürlich eine obere Schranke für die Anzahl der Lösungen über Teilkörper von $\mathbb{C}$.

Fragen zu algebraischen Gleichungen

Frage

Wie viele Lösungen hat eine algebraische Gleichung (polynomiale Gleichung) n-ten Grades?

Es kommt natürlich auf den zugrundeliegenden Körper an. Für die komplexen Zahlen haben wir:

Theorem (Fundamentalsatz der Algebra - Gauss)

Jedes nichtkonstante Polynom mit komplexen Koeffizienten besitzt mindestens eine komplexe Nullstelle.

Bemerkung

Ist Grundlage vieler Überlegungen die wir dieses Semester anstellen werden.

Fragen zu algebraischen Gleichungen

Frage

Wie viele Lösungen hat eine algebraische Gleichung (polynomiale Gleichung) n-ten Grades?

Es kommt natürlich auf den zugrundeliegenden Körper an. Für die komplexen Zahlen haben wir:

Theorem (Fundamentalsatz der Algebra - Gauss)

Jedes nichtkonstante Polynom mit komplexen Koeffizienten besitzt mindestens eine komplexe Nullstelle.

Bemerkung

Einen relativ einfachen Beweis findet man in Kapitel 19 im Buch der Beweise.

Lösung von Gleichungen durch Radikale I

Lösung von Gleichungen durch Radikale I

Frage

Gibt es explizite Lösungsformeln mit elementaren Operationen für algebraische Gleichungen beliebigen Grades?

Lösung von Gleichungen durch Radikale I

Frage

Gibt es explizite Lösungsformeln mit elementaren Operationen für algebraische Gleichungen beliebigen Grades?

Antwort

Lösung von Gleichungen durch Radikale I

Frage

Gibt es explizite Lösungsformeln mit elementaren Operationen für algebraische Gleichungen beliebigen Grades?

Antwort

Für Gleichungen von Grad kleiner gleich 4 gibt es solche Lösungsformeln, also eine Lösung durch Radikale.

Lösung von Gleichungen durch Radikale I

Frage

Gibt es explizite Lösungsformeln mit elementaren Operationen für algebraische Gleichungen beliebigen Grades?

Antwort

Für Gleichungen von Grad kleiner gleich 4 gibt es solche Lösungsformeln, also eine Lösung durch Radikale.
Für Gleichungen von Grad 5 gilt aber der folgende Satz, den wir hoffentlich gegen Ende des Semesters im Rahmen der Algebra-Vorlesung noch beweisen können.

Lösung von Gleichungen durch Radikale II

Lösung von Gleichungen durch Radikale II

Theorem

Die allgemeine algebraische Gleichung von Grad n ist nicht durch Radikale auflösbar für $n \geq 5$.

Lösung von Gleichungen durch Radikale II

Theorem

Die allgemeine algebraische Gleichung von Grad n ist nicht durch Radikale auflösbar für $n \geq 5$.

Beweisidee

Lösung von Gleichungen durch Radikale II

Theorem

Die allgemeine algebraische Gleichung von Grad n ist nicht durch Radikale auflösbar für $n \geq 5$.

Beweisidee

Wir führen das Konzept einer Galoisgruppe ein und was es für eine Gruppe heißt auflösbar zu sein. Wir werden zuerst zeigen: Sei $K \subset \mathbb{C}$ ein Körper und $p(x)$ ein Polynom in $K[x]$ mit Zerfällungskörper N. Wenn $p(x)$ auflösbar durch Radikale ist, dann ist $G := \mathrm{Gal}(N/K)$ eine auflösbare Gruppe.

Lösung von Gleichungen durch Radikale II

Theorem

Die allgemeine algebraische Gleichung von Grad n ist nicht durch Radikale auflösbar für $n \geq 5$.

Beweisidee

Wir führen das Konzept einer Galoisgruppe ein und was es für eine Gruppe heißt auflösbar zu sein. Wir werden zuerst zeigen: Sei $K \subset \mathbb{C}$ ein Körper und $p(x)$ ein Polynom in $K[x]$ mit Zerfällungskörper N. Wenn $p(x)$ auflösbar durch Radikale ist, dann ist $G := \mathrm{Gal}(N/K)$ eine auflösbare Gruppe.
Dann zeigen wir, dass für eine allgemeine Gleichung von Grad n die oben beschriebene Galoisgruppe G isomorph zur symmetrischen Gruppe S_n ist. Es bleibt uns also nur mehr zu zeigen, dass die S_n für $n \geq 5$ nicht auflösbar ist.

Lösung von Gleichungen durch Radikale III

Lösung von Gleichungen durch Radikale III

Fundamentale Konzepte die für die Lösung des Problems entwickelt wurden

Lösung von Gleichungen durch Radikale III

Fundamentale Konzepte die für die Lösung des Problems entwickelt wurden

i) Formale Definition einer Gruppe und diverse Gruppeneigenschaften,

Lösung von Gleichungen durch Radikale III

Fundamentale Konzepte die für die Lösung des Problems entwickelt wurden

i) Formale Definition einer Gruppe und diverse Gruppeneigenschaften,

ii) Galoistheorie.

Konstruktion mit Zirkel und Lineal I

Konstruktion mit Zirkel und Lineal I

Frage

Kann man ein reguläres n-Eck mit Zirkel und Lineal konstruieren?

Konstruktion mit Zirkel und Lineal I

Frage

Kann man ein reguläres n-Eck mit Zirkel und Lineal konstruieren?

Antwort

Konstruktion mit Zirkel und Lineal I

Frage

Kann man ein reguläres n-Eck mit Zirkel und Lineal konstruieren?

Antwort

Die Antwort hängt vom vorgegebenen n ab.

Konstruktion mit Zirkel und Lineal I

Frage

Kann man ein reguläres n-Eck mit Zirkel und Lineal konstruieren?

Antwort

Die Antwort hängt vom vorgegebenen n ab.

Definition

Ein Primzahl der Form $2^s + 1$ mit $s \in \mathbb{N}$ heißt *Fermat'sche Primzahl*.

Konstruktion mit Zirkel und Lineal II

Konstruktion mit Zirkel und Lineal II

Theorem

Für $3 \leq n \in \mathbb{N}$ sind äquivalent:

i) Ein reguläres n-Eck ist mit Zirkel und Lineal konstruierbar.

ii) $\phi(n)$ ist eine Potenz von 2.

iii) $n = 2^j p_1 \cdots p_r$ mit $j \in \mathbb{N}_0$ und verschiedenen fermatschen Primzahlen $p_1, \ldots, p_r$.

Konstruktion mit Zirkel und Lineal II

Theorem

Für $3 \leq n \in \mathbb{N}$ sind äquivalent:

i) Ein reguläres n-Eck ist mit Zirkel und Lineal konstruierbar.

ii) $\phi(n)$ ist eine Potenz von 2.

iii) $n = 2^j p_1 \cdots p_r$ mit $j \in \mathbb{N}_0$ und verschiedenen fermatschen Primzahlen $p_1, \ldots, p_r$.

Der Beweise dieses Satzes benutzt die Galoistheorie von Kreisteilungskörpern.

Konstruktion mit Zirkel und Lineal II

Theorem

Für $3 \leq n \in \mathbb{N}$ sind äquivalent:

i) Ein reguläres n-Eck ist mit Zirkel und Lineal konstruierbar.

ii) $\phi(n)$ ist eine Potenz von 2.

iii) $n = 2^j p_1 \cdots p_r$ mit $j \in \mathbb{N}_0$ und verschiedenen fermatschen Primzahlen $p_1, \ldots, p_r$.

Der Beweise dieses Satzes benutzt die Galoistheorie von Kreisteilungskörpern. Wir sollten bis zum Ende dieses Semester in der Lage diesen Satz vollständig zu zeigen.

Fragen zu ganzzahligen Lösungen von Gleichungen

Fragen zu ganzzahligen Lösungen von Gleichungen

Definition

Eine *Diophantische Gleichung* ist eine polynomiale Gleichung $P(x_1, \ldots, x_n) = 0$, wobei das Polynom P ganzzahlige Koeffizienten hat und man ist interessiert an ganzzahligen Lösungen für diese Gleichung.

Fragen zu ganzzahligen Lösungen von Gleichungen

Definition

Eine *Diophantische Gleichung* ist eine polynomiale Gleichung $P(x_1, \ldots, x_n) = 0$, wobei das Polynom P ganzzahlige Koeffizienten hat und man ist interessiert an ganzzahligen Lösungen für diese Gleichung.

Beispiel: Diophantische Gleichungen in einer Variablen

Sei $a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$ eine Gleichung mit ganzzahligen Koeffizienten, welche eine rationale Zahl $\frac{p}{q}$ (in gekürzter Form) als eine ihrer Lösungen hat. Dann gilt $p \mid a_n$ und $q \mid a_0$. Also müssen wir nur mehr eine endliche Liste von Möglichkeiten abarbeiten um alle ganzzahligen Lösungen dieser Gleichung zu erhalten.

Pell'sche Gleichungen

Pell'sche Gleichungen

Pell'sche Gleichungen

Eine *Pell'sche Gleichung* ist eine Diophantische Gleichung der Form

$$x^2 - 1 = dy^2.$$

Pell'sche Gleichungen

Pell'sche Gleichungen

Eine *Pell'sche Gleichung* ist eine Diophantische Gleichung der Form

$$x^2 - 1 = dy^2.$$

i) $\sqrt{2}$ irrational, daraus folgt $x^2 - 2y^2 \neq 0$ für $x, y \in \mathbb{Z}$.

Pell'sche Gleichungen

Pell'sche Gleichungen

Eine *Pell'sche Gleichung* ist eine Diophantische Gleichung der Form

$$x^2 - 1 = dy^2.$$

i) $\sqrt{2}$ irrational, daraus folgt $x^2 - 2y^2 \neq 0$ für $x, y \in \mathbb{Z}$.
ii) Frage: Wie kann man $\sqrt{2}$ möglichst gut mit einer rationalen Zahl approximieren?

Pell'sche Gleichungen

Pell'sche Gleichungen

Eine *Pell'sche Gleichung* ist eine Diophantische Gleichung der Form

$$x^2 - 1 = dy^2.$$

i) $\sqrt{2}$ irrational, daraus folgt $x^2 - 2y^2 \neq 0$ für $x, y \in \mathbb{Z}$.
ii) Frage: Wie kann man $\sqrt{2}$ möglichst gut mit einer rationalen Zahl approximieren?
iii) Oder anders formuliert: Gibt es ganzzahlige Lösungen der Gleichung $x^2 - 2y^2 = \pm 1$?

Pell'sche Gleichungen

Pell'sche Gleichungen

Eine *Pell'sche Gleichung* ist eine Diophantische Gleichung der Form

$$x^2 - 1 = dy^2.$$

i) $\sqrt{2}$ irrational, daraus folgt $x^2 - 2y^2 \neq 0$ für $x, y \in \mathbb{Z}$.
ii) Frage: Wie kann man $\sqrt{2}$ möglichst gut mit einer rationalen Zahl approximieren?
iii) Oder anders formuliert: Gibt es ganzzahlige Lösungen der Gleichung $x^2 - 2y^2 = \pm 1$?
iv) 2 Fälle: für $+1$, gibt es viele ganzzahlige Lösungen (kann man mit Rekursionsformeln finden); für -1 gibt es keine ganzzahligen Lösungen.

Pell'sche Gleichungen

Pell'sche Gleichungen

Eine *Pell'sche Gleichung* ist eine Diophantische Gleichung der Form

$$x^2 - 1 = dy^2.$$

i) $\sqrt{2}$ irrational, daraus folgt $x^2 - 2y^2 \neq 0$ für $x, y \in \mathbb{Z}$.
ii) Frage: Wie kann man $\sqrt{2}$ möglichst gut mit einer rationalen Zahl approximieren?
iii) Oder anders formuliert: Gibt es ganzzahlige Lösungen der Gleichung $x^2 - 2y^2 = \pm 1$?
iv) 2 Fälle: für $+1$, gibt es viele ganzzahlige Lösungen (kann man mit Rekursionsformeln finden); für -1 gibt es keine ganzzahligen Lösungen.
v) Zusammenhang zw. Lösungen der Gleichung $x^2 - dy^2 = \pm 1$ und der Einheitengruppe von $\mathbb{Z}[\sqrt{d}]$.

Frage

Hat die Gleichung $y^3 = x^2 + 2$ eine positive ganzzahlige Lösung?

Frage

Hat die Gleichung $y^3 = x^2 + 2$ eine positive ganzzahlige Lösung?

Theorem (Euler 1770)

Das Paar $(5, 3)$ ist die einzige Lösung welche die obige Bed. erfüllt.

Frage

Hat die Gleichung $y^3 = x^2 + 2$ eine positive ganzzahlige Lösung?

Theorem (Euler 1770)

Das Paar $(5, 3)$ ist die einzige Lösung welche die obige Bed. erfüllt.

Proof.

Wir können schreiben: $y^3 = (x + \sqrt{-2})(x - \sqrt{-2}) = x^2 + 2$. Wenn sich die Zahlen $a + b\sqrt{-2}$ mit $a, b \in \mathbb{Z}$ wie die Zahlen in $\mathbb{Z}$ verhalten (wenn $\mathbb{Z}[\sqrt{-2}]$ faktoriell ist) muss gelten $(x + \sqrt{-2}) = (a + b\sqrt{2})^3$. Daraus folgt, das $x = \pm 5$ sein muss, also $y = 3$. □

Frage

Hat die Gleichung $y^3 = x^2 + 2$ eine positive ganzzahlige Lösung?

Theorem (Euler 1770)

Das Paar $(5, 3)$ ist die einzige Lösung welche die obige Bed. erfüllt.

Proof.

Wir können schreiben: $y^3 = (x + \sqrt{-2})(x - \sqrt{-2}) = x^2 + 2$. Wenn sich die Zahlen $a + b\sqrt{-2}$ mit $a, b \in \mathbb{Z}$ wie die Zahlen in $\mathbb{Z}$ verhalten (wenn $\mathbb{Z}[\sqrt{-2}]$ faktoriell ist) muss gelten $(x + \sqrt{-2}) = (a + b\sqrt{2})^3$. Daraus folgt, das $x = \pm 5$ sein muss, also $y = 3$. □

Bemerkung

Eines der Ziele unserer Veranstaltung ist es präzise zu machen, was es heißt, dass sich Elemente eines Rings (wie der Ring $\mathbb{Z}[\sqrt{-2}]$) sich so 'verhalten' wie Elemente aus $\mathbb{Z}$. Danach können wir den obigen Beweis auch nach heutigen Standards korrekt formulieren.

Der Ring $\mathbb{Z}[\sqrt{-5}]$

Der Ring $\mathbb{Z}[\sqrt{-5}]$

Sei $\alpha \in \mathbb{Z}[\sqrt{-5}] \in \mathbb{C}$ und $N(\alpha) := \alpha\overline{\alpha}$ die Normabbildung. Ein Element α ist *prim*, wenn $N(\alpha) > 1$ und es kein Produktdarstellung mit Elementen in $\mathbb{Z}[\sqrt{-5}]$ von kleinerer Norm gibt.

Der Ring $\mathbb{Z}[\sqrt{-5}]$

Sei $\alpha \in \mathbb{Z}[\sqrt{-5}] \in \mathbb{C}$ und $N(\alpha) := \alpha\overline{\alpha}$ die Normabbildung. Ein Element α ist *prim*, wenn $N(\alpha) > 1$ und es kein Produktdarstellung mit Elementen in $\mathbb{Z}[\sqrt{-5}]$ von kleinerer Norm gibt.
Jedes Element von $\mathbb{Z}[\sqrt{-5}]$ faktorisiert in Primelemente von $\mathbb{Z}[\sqrt{-5}]$. Die Faktorisierung ist aber nicht mehr eindeutig, zum Beispiel gilt
$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

Der Ring $\mathbb{Z}[\sqrt{-5}]$

Sei $\alpha \in \mathbb{Z}[\sqrt{-5}] \in \mathbb{C}$ und $N(\alpha) := \alpha\overline{\alpha}$ die Normabbildung. Ein Element α ist *prim*, wenn $N(\alpha) > 1$ und es kein Produktdarstellung mit Elementen in $\mathbb{Z}[\sqrt{-5}]$ von kleinerer Norm gibt.
Jedes Element von $\mathbb{Z}[\sqrt{-5}]$ faktorisiert in Primelemente von $\mathbb{Z}[\sqrt{-5}]$. Die Faktorisierung ist aber nicht mehr eindeutig, zum Beispiel gilt
$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

Idee von Kummer: 'ideale Zahlen' bzw. Ideale sollen eind. Primfaktorenzerlegung erhalten. Dedekind definiert 1871 Ideale präzise.

Der Ring $\mathbb{Z}[\sqrt{-5}]$

Sei $\alpha \in \mathbb{Z}[\sqrt{-5}] \in \mathbb{C}$ und $N(\alpha) := \alpha\overline{\alpha}$ die Normabbildung. Ein Element α ist *prim*, wenn $N(\alpha) > 1$ und es kein Produktdarstellung mit Elementen in $\mathbb{Z}[\sqrt{-5}]$ von kleinerer Norm gibt.
Jedes Element von $\mathbb{Z}[\sqrt{-5}]$ faktorisiert in Primelemente von $\mathbb{Z}[\sqrt{-5}]$. Die Faktorisierung ist aber nicht mehr eindeutig, zum Beispiel gilt
$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

Idee von Kummer: 'ideale Zahlen' bzw. Ideale sollen eind. Primfaktorenzerlegung erhalten. Dedekind definiert 1871 Ideale präzise.
Einen kleinen Teil der seither entwickelten Idealtheorie für kommutative Ringe werden wir im Laufe unserer Veranstaltungen kennenlernen.

Fermat'sche Vermutung

Fermat'sche Vermutung

Theorem (Fermat'sche Vermutung (FLT) - Theorem von Wiles (1995))

Die Gleichung $x^n + y^n = z^n$ *hat keine Lösung, wenn* $x, y, z \in \mathbb{Z}$, $xyz \neq 0$ *und* $n > 2$.

Fermat'sche Vermutung

Theorem (Fermat'sche Vermutung (FLT) - Theorem von Wiles (1995))

Die Gleichung $x^n + y^n = z^n$ *hat keine Lösung, wenn* $x, y, z \in \mathbb{Z}$, $xyz \neq 0$ *und* $n > 2$.

Eine Highlights aus der Geschichte dieses Theorems:

Fermat'sche Vermutung

Theorem (Fermat'sche Vermutung (FLT) - Theorem von Wiles (1995))

Die Gleichung $x^n + y^n = z^n$ hat keine Lösung, wenn $x, y, z \in \mathbb{Z}$, $xyz \neq 0$ und $n > 2$.

Eine Highlights aus der Geschichte dieses Theorems:

i) $\sim$ 1630 Fermat beweist den Satz für $n = 4$ und zeigt, es reicht die Fälle zu betrachten, wenn n eine ungerade Primzahl ist und x, y, z relativ prim sind.

Fermat'sche Vermutung

Theorem (Fermat'sche Vermutung (FLT) - Theorem von Wiles (1995))

Die Gleichung $x^n + y^n = z^n$ hat keine Lösung, wenn $x, y, z \in \mathbb{Z}$, $xyz \neq 0$ und $n > 2$.

Eine Highlights aus der Geschichte dieses Theorems:

i) $\sim$ 1630 Fermat beweist den Satz für $n = 4$ und zeigt, es reicht die Fälle zu betrachten, wenn n eine ungerade Primzahl ist und x, y, z relativ prim sind.

ii) 1729: Goldbach schreibt an Euler dieses Problem, Euler beginnt sich für Zahlentheorie zu interessieren.

Fermat'sche Vermutung

Theorem (Fermat'sche Vermutung (FLT) - Theorem von Wiles (1995))

Die Gleichung $x^n + y^n = z^n$ hat keine Lösung, wenn $x, y, z \in \mathbb{Z}$, $xyz \neq 0$ und $n > 2$.

Eine Highlights aus der Geschichte dieses Theorems:

i) $\sim$ 1630 Fermat beweist den Satz für $n = 4$ und zeigt, es reicht die Fälle zu betrachten, wenn n eine ungerade Primzahl ist und x, y, z relativ prim sind.

ii) 1729: Goldbach schreibt an Euler dieses Problem, Euler beginnt sich für Zahlentheorie zu interessieren.

iii) 1825: Dirichlet und Legendre zeigen den Fall $n = 5$.

Fermat'sche Vermutung

Theorem (Fermat'sche Vermutung (FLT) - Theorem von Wiles (1995))

Die Gleichung $x^n + y^n = z^n$ hat keine Lösung, wenn $x, y, z \in \mathbb{Z}$, $xyz \neq 0$ und $n > 2$.

Eine Highlights aus der Geschichte dieses Theorems:

i) $\sim$ 1630 Fermat beweist den Satz für $n = 4$ und zeigt, es reicht die Fälle zu betrachten, wenn n eine ungerade Primzahl ist und x, y, z relativ prim sind.

ii) 1729: Goldbach schreibt an Euler dieses Problem, Euler beginnt sich für Zahlentheorie zu interessieren.

iii) 1825: Dirichlet und Legendre zeigen den Fall $n = 5$.

iv) 1847: falscher Beweis für allgemeine n wird von Cauchy und Lame vorgelegt

v) $\sim$ 1845 Kummer arbeitet an dem Problem. Idee:

$$x^p = z^p - y^p = \prod_{j=0}^{p-1} (z - \zeta_p^j)$$

mit $\zeta_p = e^{2\pi i/p}$ Einheitswurzel mit $\zeta_p^p = 1$. Auf der Menge der zyklotomischen ganzen Zahlen $\mathbb{Z}[\zeta_p]$ lässt sich eine natürliche Ringstruktur definieren. Problem des Ansatzes ist aber: in einigen Fällen gibt es keine eindeutige Primzerlegung zB bei $p = 23$. Zwei Lösungsansätze von Kummer für dieses Problem: Verallgemeinerung der zykl. ganzen Zahlen $\Rightarrow$ 'ideale Zahlen' bzw. Ideale
'Messen' wie viel auf die eindeutige Faktorisierung fehlt $\Rightarrow$ Klassenzahl h. Das kann man als die 'Geburtsstunde' der Algebraischen Zahlentheorie betrachten.

v) $\sim$ 1845 Kummer arbeitet an dem Problem. Idee:

$$x^p = z^p - y^p = \prod_{j=0}^{p-1} (z - \zeta_p^j)$$

mit $\zeta_p = e^{2\pi i/p}$ Einheitswurzel mit $\zeta_p^p = 1$. Auf der Menge der zyklotomischen ganzen Zahlen $\mathbb{Z}[\zeta_p]$ lässt sich eine natürliche Ringstruktur definieren. Problem des Ansatzes ist aber: in einigen Fällen gibt es keine eindeutige Primzerlegung zB bei $p = 23$. Zwei Lösungsansätze von Kummer für dieses Problem: Verallgemeinerung der zykl. ganzen Zahlen $\Rightarrow$ 'ideale Zahlen' bzw. Ideale
'Messen' wie viel auf die eindeutige Faktorisierung fehlt $\Rightarrow$ Klassenzahl h. Das kann man als die 'Geburtsstunde' der Algebraischen Zahlentheorie betrachten.

vi) 1847: Kummer zeigt FLT für p wenn $p \nmid h$ gilt (reguläre Primzahlen).

vii) 1983: Faltings zeigt Mordell'sche Vermutung, diese impliziert eine Polynomialgleichung $P(x, y) = 0$ mit rationalen Koeffizienten hat nur endlich viele Lösungen, wenn die zugehörige Kurve Genus größer gleich 2 hat. Da $x^n + y^n = 1$ Genus ≥ 2 hat für $n \geq 2$, hat die Gleichung nur endlich viele rationale Lösungen. Wegmultiplizieren der Nenner liefert, dass auch $x^n + y^n = y^n$ nur endlich viele Lösungen hat.

vii) 1983: Faltings zeigt Mordell'sche Vermutung, diese impliziert eine Polynomialgleichung $P(x, y) = 0$ mit rationalen Koeffizienten hat nur endlich viele Lösungen, wenn die zugehörige Kurve Genus größer gleich 2 hat. Da $x^n + y^n = 1$ Genus ≥ 2 hat für $n \geq 2$, hat die Gleichung nur endlich viele rationale Lösungen. Wegmultiplizieren der Nenner liefert, dass auch $x^n + y^n = y^n$ nur endlich viele Lösungen hat.

viii) Es gelingt zu zeigen, dass die Taniyama-Shimura Vermutung, also die Aussage, dass jede elliptische Kurve über $\mathbb{Q}$ modular ist, impliziert FLT für alle.

vii) 1983: Faltings zeigt Mordell'sche Vermutung, diese impliziert eine Polynomialgleichung $P(x, y) = 0$ mit rationalen Koeffizienten hat nur endlich viele Lösungen, wenn die zugehörige Kurve Genus größer gleich 2 hat. Da $x^n + y^n = 1$ Genus ≥ 2 hat für $n \geq 2$, hat die Gleichung nur endlich viele rationale Lösungen. Wegmultiplizieren der Nenner liefert, dass auch $x^n + y^n = y^n$ nur endlich viele Lösungen hat.

viii) Es gelingt zu zeigen, dass die Taniyama-Shimura Vermutung, also die Aussage, dass jede elliptische Kurve über $\mathbb{Q}$ modular ist, impliziert FLT für alle.

ix) 1995: A. Wiles zeigt einen Spezialfall der Taniyama-Shimura Vermutung der aussreicht um FLT für alle Exponenten zu zeigen.

vii) 1983: Faltings zeigt Mordell'sche Vermutung, diese impliziert eine Polynomialgleichung $P(x, y) = 0$ mit rationalen Koeffizienten hat nur endlich viele Lösungen, wenn die zugehörige Kurve Genus größer gleich 2 hat. Da $x^n + y^n = 1$ Genus ≥ 2 hat für $n \geq 2$, hat die Gleichung nur endlich viele rationale Lösungen. Wegmultiplizieren der Nenner liefert, dass auch $x^n + y^n = y^n$ nur endlich viele Lösungen hat.

viii) Es gelingt zu zeigen, dass die Taniyama-Shimura Vermutung, also die Aussage, dass jede elliptische Kurve über $\mathbb{Q}$ modular ist, impliziert FLT für alle.

ix) 1995: A. Wiles zeigt einen Spezialfall der Taniyama-Shimura Vermutung der aussreicht um FLT für alle Exponenten zu zeigen.

x) 2001: Breuil, Conrad, Diamond und Taylor beweisen die Taniyama-Shimura Vermutung vollständig.

Elkies Gleichung

Elkies Gleichung

Frage

Hat die Diophantische Gleichung $x^4 + y^4 + z^4 = w^4$ eine Lösung?

Elkies Gleichung

Frage

Hat die Diophantische Gleichung $x^4 + y^4 + z^4 = w^4$ eine Lösung?

Euler vermutete das es keine ganzzahlige Lösung gibt.

Elkies Gleichung

Frage

Hat die Diophantische Gleichung $x^4 + y^4 + z^4 = w^4$ eine Lösung?

Euler vermutete das es keine ganzzahlige Lösung gibt.

Antwort

Ja, es gibt eine Lösung. 1988 hat Noam Elkies gezeigt

$$2682440^4 + 15365639^4 + 19796760^4 = 20615673^4.$$

Elkies Gleichung

Frage

Hat die Diophantische Gleichung $x^4 + y^4 + z^4 = w^4$ eine Lösung?

Euler vermutete das es keine ganzzahlige Lösung gibt.

Antwort

Ja, es gibt eine Lösung. 1988 hat Noam Elkies gezeigt

$$2682440^4 + 15365639^4 + 19796760^4 = 20615673^4.$$

Moral: Auch großartige Mathematiker können einmal falsch liegen.

Homer Simpson trifft Fermat

Homer Simpson trifft Fermat

In der TV-Serie 'Die Simpsons' ist in einer Folge ein 'Gegenbeispiel' zur Fermat'schen Vermutung zu sehen: Gibt man in einen Taschenrechner $(1782^{12} + 1841^{12})^{1/12}$ ein erhält man 1922 und somit wäre ein Gegenbeispiel gefunden.

Homer Simpson trifft Fermat

In der TV-Serie 'Die Simpsons' ist in einer Folge ein 'Gegenbeispiel' zur Fermat'schen Vermutung zu sehen: Gibt man in einen Taschenrechner $(1782^{12} + 1841^{12})^{1/12}$ ein erhält man 1922 und somit wäre ein Gegenbeispiel gefunden.

Was stimmt mit dem 'Gegenbeispiel' nicht?

Homer Simpson trifft Fermat

In der TV-Serie 'Die Simpsons' ist in einer Folge ein 'Gegenbeispiel' zur Fermat'schen Vermutung zu sehen: Gibt man in einen Taschenrechner $(1782^{12} + 1841^{12})^{1/12}$ ein erhält man 1922 und somit wäre ein Gegenbeispiel gefunden.

Was stimmt mit dem 'Gegenbeispiel' nicht?

Das Resultat ist genügend Stellen korrekt, damit ein Taschenrechner reingelegt wird. Es gilt

$$(1782^{12} + 1841^{12})^{1/12} = 1921,999999958672254.$$

Homer Simpson trifft Fermat

In der TV-Serie 'Die Simpsons' ist in einer Folge ein 'Gegenbeispiel' zur Fermat'schen Vermutung zu sehen: Gibt man in einen Taschenrechner $(1782^{12} + 1841^{12})^{1/12}$ ein erhält man 1922 und somit wäre ein Gegenbeispiel gefunden.

Was stimmt mit dem 'Gegenbeispiel' nicht?

Das Resultat ist genügend Stellen korrekt, damit ein Taschenrechner reingelegt wird. Es gilt

$$(1782^{12} + 1841^{12})^{1/12} = 1921,999999958672254.$$

Moral: Taschenrechner müssen in der Mathematik nicht immer hilfreich sein.

Hilbert's 10. Problem

Hilbert's 10. Problem

Frage

Gibt es einen allgemeinen Algorithmus der entscheidet ob eine gegebene Diophantische Gleichung eine Lösung hat oder nicht?

Hilbert's 10. Problem

Frage

Gibt es einen allgemeinen Algorithmus der entscheidet ob eine gegebene Diophantische Gleichung eine Lösung hat oder nicht?

Das ist die 10. Frage von Hilbert's Problemliste aus dem Jahr 1900.

Hilbert's 10. Problem

Frage

Gibt es einen allgemeinen Algorithmus der entscheidet ob eine gegebene Diophantische Gleichung eine Lösung hat oder nicht?

Das ist die 10. Frage von Hilbert's Problemliste aus dem Jahr 1900.

Antwort

Nein. Bewiesen von Yu. Matiyasevich der auf Arbeiten von M. Davis, H. Putnam and J. Robinson aufbaute. Der Beweis basiert auf einer speziellen Art des 'Zählens': es stellt sich heraus, dass es 'mehr' Diophantische Mengen gibt als berechenbare Mengen.

Offene Probleme

Offene Probleme

Braucht jemand 75.000 Dollar?

Offene Probleme

Braucht jemand 75.000 Dollar?

Man muss nur die Zahl
412023436986659543855531365332575948179811699844
327982845455626433876445565248426198098870423161
841879261420247188869492560931776375033421130982
397485150944909106910269861031862704114880866970
564902903653658867433731720813104105190864254793
282601391257624033946373269391 faktorisieren.

Offene Probleme

Braucht jemand 75.000 Dollar?

Man muss nur die Zahl
412023436986659543855531365332575948179811699844
327982845455626433876445565248426198098870423161
841879261420247188869492560931776375033421130982
397485150944909106910269861031862704114880866970
564902903653658867433731720813104105190864254793
282601391257624033946373269391 faktorisieren.

Gibt es Lösungen zu folgenden Diophantischen Gleichungen?

Offene Probleme

Braucht jemand 75.000 Dollar?

Man muss nur die Zahl
412023436986659543855531365332575948179811699844
327982845455626433876445565248426198098870423161
841879261420247188869492560931776375033421130982
397485150944909106910269861031862704114880866970
564902903653658867433731720813104105190864254793
282601391257624033946373269391 faktorisieren.

Gibt es Lösungen zu folgenden Diophantischen Gleichungen?

i) $x^6 + y^6 + z^6 + u^6 + v^6 = w^6$,

ii) $x^5 + y^5 + z^5 = w^5$,

iii) $x^k + y^k = n!z^k$, mit $k \geq 2$, $n > 1$,...

iv) $x^a + y^b = z^c$, mit $a, b, c > 2$ und $\mathrm{ggT}(a, b, c) = 1$.

Aufgabe bis Ende des Semesters

Lösen Sie eines der offenen Probleme der elementaren Zahlentheorie (der obigen oder ein anderes) und entwickeln Sie im Zuge davon ein neues algebraisches Konzept.