INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

21. Oktober 2004

Einführung in die Zahlentheorie

1. Übungsblatt

Abgabe vor der nächsten Übung

Aufgabe 1 (*5+5 Punkte*)

Zeigen Sie, dass für alle $n \in \mathbb{N}$ gilt:

(a) $15 \mid (2^{4n} - 1)$

(b) $720 \mid (n^2 + 3n)(n^2 - 1)(n^2 - 4)$

Aufgabe 2 (*10 Punkte*)

Berechnen Sie den größten gemeinsamen Teiler der Zahlen $a := 8091$ und $b := 5425$ und stellen Sie $\mathrm{ggT}(a, b)$ als ganzzahlige Linearkombination von a und b dar. Untersuchen Sie für $c = 99$ und $c = 341$ jeweils, ob die diophantische Gleichung $ax + by = c$ lösbar ist und bestimmen Sie gegebenenfalls sämtliche Lösungen.

Aufgabe 3*

Zeigen Sie: $(a, b) = 1 \Rightarrow (a + b, a - b) \in \{1, 2\}$

Aufgabe 4*

Beweisen Sie das folgende Teilbarkeitskriterium:

Es sei $n \geq 10$ eine natürliche Zahl, gegeben in Dezimaldarstellung. Streicht man die letzte Ziffer von n und subtrahiert sie zweimal von der derart „verkürzten" Zahl (Beispiel: aus 376 wird $37 - 2 \cdot 6 = 25$), so ist das Ergebnis genau dann durch 7 teilbar, wenn n durch 7 teilbar ist.

Für welche $k \in \mathbb{N}$ ist $a_k := 33 \ldots 331$ (k 3en, gefolgt von einer 1) durch 7 teilbar?

Hinweis: Mit einem Stern (*) versehene Aufgaben werden nicht korrigiert!

1. Stundenübung

21. Oktober 2004

Aufgabe 1

Für welche $n \in \mathbb{N} \cup \{0\}$ gilt:

(a) $3 \mid (n^3 + 2n)$

(b) $6 \mid (n^3 - n)$

(c) $(n+1) \mid (n^2 + 3)$?

Aufgabe 2

Zeigen Sie: Für alle $a, b, n \in \mathbb{N}$ gilt $(a, b) = (a, b + na)$.

Aufgabe 3

Berechnen Sie den größten gemeinsamen Teiler der Zahlen $a := 648$ und $b := 234$ und stellen Sie $\mathrm{ggT}(a, b)$ als ganzzahlige Linearkombination von a und b dar. Untersuchen Sie, ob die diophantische Gleichung $ax + by = 54$ lösbar ist und bestimmen Sie gegebenenfalls alle Lösungen.

Aufgabe 4

Bestimmen Sie $\mathrm{ggT}(n^4 + 3n^2 + 1, n^3 + 2n)$, $n \in \mathbb{N}$.

Literatur zur Zahlentheorie

- A. Baker, **Theory of numbers** , Cambridge University Press 1984
  Knappe Darstellung der Grundlagen inkl. Bemerkungen zu aktuellen Entwicklungen
- P. Bundschuh, **Einführung in die Zahlentheorie**, Springer 2002
  Ausführliche Darstellung inkl. geschichtlicher Entwicklung, reichlich Diophantische Approximation
- G.H. Hardy, E.M. Wright, **Einführung in die Zahlentheorie**, Oldenbourg 1958
  Umfangreiches Standardwerk der elementaren Zahlentheorie
- K.-H. Indlekofer, **Zahlentheorie** , Birkhäuser 1978
  Kurze Einführung mit Übungsaufgaben
- I. Niven, H.S. Zuckerman, **Einführung in die Zahlentheorie** (B.I.Wissenschaftsverlag, Band 46 und Band 47)
  Umfassende Darstellung mit Weiterführung

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

28. Oktober 2004

Einführung in die Zahlentheorie

2. Übungsblatt

Abgabe vor der nächsten Übung

Aufgabe 1 (*10 Punkte*)

Es sei $a = 5880$ und $b = 4158$. Bestimmen Sie die Primfaktorzerlegungen von a, b, $\mathrm{ggT}(a,b)$ und $\mathrm{kgV}(a,b)$. Berechnen Sie außerdem $\varphi(a)$, $\varphi(b)$, $\varphi(\mathrm{ggT}(a,b))$, $\mu(a)$, $\mu(b)$ und $\mu(\mathrm{ggT}(a,b))$.

Aufgabe 2 (*10 Punkte*)

Es sei $n \in \mathbb{N}$, $n > 1$. Zeigen Sie: n ist genau dann prim, wenn keine Primzahl $p \leq \sqrt{n}$ ein Teiler von n ist.

Prüfen Sie mit diesem Kriterium, ob $6! + 1$, $6! - 1$ und $7! + 1$ prim sind.

Aufgabe 3*

Bestimmen Sie die Anzahl der Nullen, mit denen die Dezimaldarstellung von 2004! endet.

Aufgabe 4*

Zeigen Sie:

a) $\phi(n) = \frac{n}{2} \Leftrightarrow n = 2^k, k \in \mathbb{N}$

b) Für kein $n \in \mathbb{N}$ ist $\varphi(n) = 14$.

Hinweis: Mit einem Stern (*) versehene Aufgaben werden nicht korrigiert!

2. Stundenübung

28. Oktober 2004

Aufgabe 1

Es sei $a = 7!$ und $b = 11700$. Bestimmen Sie die Primfaktorzerlegungen von a, b, $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$. Verifizieren Sie anhand der Zerlegungen, dass $(a, b) \cdot [a, b] = |ab|$ gilt.

Aufgabe 2

Bestimmen Sie die Primfaktorzerlegung von 12! mit Hilfe von Satz 2.2.

Aufgabe 3

Berechnen Sie $\varphi(n)$ für $n = 12$ sowie $n = 12!$ und bestätigen Sie im Falle $n = 12$ durch Nachrechnen, daß gilt:

- $\displaystyle\sum_{d|n} \mu(d) = 0$ (Die summatorische Funktion zu μ ist $\varepsilon(n) := \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$.)
- $\displaystyle\sum_{d|n} \varphi(d) = n$ (Die summatorische Funktion zu φ ist die Identität.)
- $\displaystyle\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$ (Möbius-Umkehrung)

Aufgabe 4

a) Für jeweils welche $n \in \mathbb{N}$ gilt $\varphi(2n) = \varphi(n)$ bzw. $\varphi(2n) = 2\varphi(n)$?

b) Zeigen Sie: Es gibt unendlich viele $n \in \mathbb{N}$, für die $\varphi(n)$ eine Quadratzahl ist.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

4. November 2004

Einführung in die Zahlentheorie

3. Übungsblatt

Abgabe vor der nächsten Übung

Aufgabe 1 (*8 Punkte*)

Nach Satz 2.10 gibt es eine eindeutig bestimmte Funktion $f : \mathbb{N} \to \mathbb{Z}$, deren summatorische Funktion genau die Eulersche φ-Funktion ist. Sie dürfen ohne Beweis benutzen, daß f multiplikativ ist.
Bestimmen Sie $f(p^k)$ für $p \in \mathbb{P}$, $k \in \mathbb{N}$, und berechnen Sie damit $f(675)$ sowie $f(2222222)$.
(*Hinweis:* Der zweite Wert läßt sich ohne Primfaktorzerlegung bestimmen.)

Aufgabe 2 (*6+2 Punkte*)

a) Berechnen Sie für $n = 119$, $n = 120$ und $n = 121$ jeweils $\tau(n)$ und $\sigma(n)$ und geben Sie an, ob n defizient, vollkommen oder abundant ist.

b) Was ist $\displaystyle\sum_{d|n} \mu(d)\,\tau(\frac{n}{d})$ für beliebiges $n \in \mathbb{N}$?

Aufgabe 3 (*4 Punkte*)

Bestimmen Sie alle ganzzahligen Vielfachen von 10, die genau 35 positive Teiler besitzen.

Aufgabe 4*

Bestimmen Sie die kleinste natürliche Zahl mit genau 100 positiven Teilern.

Aufgabe 5*

N sei eine vollkommene Zahl. Was ist dann $\displaystyle\sum_{d|N} \frac{1}{d}$?

Hinweis: Mit einem Stern (*) versehene Aufgaben werden nicht korrigiert!

3. Stundenübung

4. November 2004

Aufgabe 1

$F : \mathbb{N} \to \mathbb{N}$ sei definiert wie folgt: $F(n) = 1$, falls n Quadratzahl ist, und $F(n) = 0$ sonst.

Nach Satz 2.10 (Möbius-Umkehrung) existiert dann eine eindeutig bestimmte Funktion $\lambda : \mathbb{N} \to \mathbb{Z}$, deren summatorische Funktion F ist. Bestimmen Sie $\lambda(p^k)$ für $p \in \mathbb{P}$, $k \in \mathbb{N}$, und berechnen Sie damit $\lambda(100)$.

Hinweis: F ist multiplikativ und damit auch λ; dies dürfen Sie ohne Beweis benutzen.

Aufgabe 2

Berechnen Sie für $n = 33$ und $n = 540$ die Werte $\tau(n)$, $\sigma(n)$ und $\sum_{d|n} \mu(d)\,\sigma(\frac{n}{d})$.

Prüfen Sie jeweils, ob n defizient, vollkommen oder abundant ist.

Aufgabe 3

Zeigen Sie: Es gibt jeweils unendlich viele defiziente bzw. abundante Zahlen.

Aufgabe 4

Mersenne-Primzahlen sind Primzahlen der Form $2^n - 1$ mit $n \in \mathbb{N}$.

a) Zeigen Sie: $2^n - 1 \in \mathbb{P} \Rightarrow n \in \mathbb{P}$. (Mersenne-Primzahlen sind also sogar stets von der Form $2^p - 1$ mit p prim.)

b) Bestimmen Sie fünf vollkommene Zahlen mit Hilfe von Satz 2.14.

Korrektorin: Yvonne Steffen, Sprechstunde Mi 13-14 in D405

Übungsblätter im Netz: www.unics.uni-hannover.de/nhadschw

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

11. November 2004

Einführung in die Zahlentheorie

4. Übungsblatt

Abgabe vor der nächsten Übung

Aufgabe 1 (*8 Punkte*)

Berechnen Sie im Körper $\mathbb{Z}_{73}$: 29^{-1}, 12^{16}, $\dfrac{33^3 \cdot 44^4 + 70}{(-48) \cdot (-59)}$.

Aufgabe 2 (*12 Punkte*)

Prüfen Sie, ob folgende Kongruenzen lösbar sind und bestimmen Sie ggf. alle Lösungen:

(a) $42x \equiv 28 \mod 49$

(b) $100x \equiv 59 \mod 3$

(c) $135x \equiv 833 \mod 1001$

(d) $987x \equiv 610 \mod 1597$

Aufgabe 3*

(a) $f(x)$ sei ein Polynom vom Grad n. Zeigen Sie: $f(x) = O(x^n)$, $x \to \infty$.

(b) Zeigen Sie, daß für jedes $\varepsilon > 0$ gilt: $\tau(n) = o(n^\varepsilon)$, $n \to \infty$. (*Hinweis:* Satz 2.15)

Aufgabe 4*

(a) Es sei n eine natürliche Zahl mit Dezimaldarstellung $n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_0$. Dann heißt $\tilde{Q}(n) := \sum_{i=0}^{k} (-1)^i a_i$ die *alternierende Quersumme* von n. Zeigen Sie: $11 \mid n \Leftrightarrow 11 \mid \tilde{Q}(n)$.

(b) Formulieren Sie ein Kriterium, mit dem sich anhand der Dezimaldarstellung von n entscheiden läßt, ob n durch 37 teilbar ist. Prüfen Sie, ob die 999-stellige Zahl $n = 222\ldots2$ durch 3, 9, 11 oder 37 teilbar ist.

Aufgabe 5*

(a) Zeigen Sie, daß $3^a + 3^b + 1$ für $a, b \in \mathbb{N}$ niemals eine Quadratzahl ist.

(b) Zeigen Sie, daß die diophantische Gleichung $x^4 + 4y^4 = z^4 + 2$ keine Lösung besitzt.

Hinweis: Arbeiten Sie für (a) modulo 8 und versuchen Sie bei (b) einen ähnlichen Trick.

Mit einem Stern (*) versehene Aufgaben werden nicht korrigiert!

4. Stundenübung

11. November 2004

Aufgabe 1

Zeigen Sie:

a) $1 + 2 + 3 + \cdots + n = \frac{1}{2}n^2 + O(n) \quad (n \to \infty)$

b) $O(x) + O(x^2) = O(x^2)$, $x \to \infty$

c) Für jedes $\varepsilon > 0$ gilt: $O(x^k) = o(x^{k+\varepsilon})$, $x \to \infty$.

Aufgabe 2

(a) Bestimmen Sie für jede der folgenden Zahlen den kleinsten nichtnegativen Repräsentanten ihrer Restklasse modulo 7: -1, 2004, 2^{99}, $6!, 1! + 2! + 3! + \cdots + 100!$

(b) Geben Sie die multiplikative Verknüpfungstafel des Restklassenringes $\mathbb{Z}_6$ an. Zu welchen $a \in \mathbb{Z}_6$ existiert ein inverses Element bzgl. Multiplikation?

(c) Für $p \in \mathbb{P}$ ist der Restklassenring $\mathbb{Z}_p$ sogar ein Körper. Bestätigen Sie dies für $p = 7$ explizit, indem Sie zu jedem $a \in \mathbb{Z}_7 \backslash \{0\}$ das inverse Element a^{-1} bestimmen. Berechnen Sie im Körper $\mathbb{Z}_7$ den Quotienten $5^6/4^9$.

Aufgabe 3

Bestimmen Sie alle Lösungen der folgenden linearen Kongruenzen:

(a) $15x \equiv 9 \mod 25$, (b) $15x \equiv 9 \mod 27$, (c) $8x \equiv 2 \mod 101$, (d) $99x \equiv 13 \mod 1000$

Aufgabe 4

Es sei n eine natürliche Zahl mit der Dezimaldarstellung $n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_0$, $a_i \in \{0, 1, \ldots, 9\}$ für $0 \leq i \leq k$. Dann heißt $Q(n) := \sum_{i=0}^{k} a_i$ die *Quersumme* von n.
Zeigen Sie: $3 \mid n \Leftrightarrow 3 \mid Q(n)$, und $9 \mid n \Leftrightarrow 9 \mid Q(n)$.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

18. November 2004

Einführung in die Zahlentheorie

5. Übungsblatt

Abgabe vor der nächsten Übung

Aufgabe 1 (*9 Punkte*)

Prüfen Sie, ob die folgenden Kongruenzsysteme lösbar sind und bestimmen Sie ggf. alle Lösungen:

(a) $\begin{cases} 4x \equiv 3 \bmod 7 \\ 14x \equiv 8 \bmod 20 \\ 7x \equiv 2 \bmod 9 \end{cases}$ (b) $\begin{cases} x \equiv 2 \bmod 6 \\ x \equiv 4 \bmod 8 \\ x \equiv 2 \bmod 14 \\ x \equiv 5 \bmod 9 \end{cases}$ (c) $\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 4 \\ \dots \\ x \equiv 9 \bmod 10 \end{cases}$

Aufgabe 2 (*7+4 Punkte*)

(a) Bestimmen Sie für jedes a mit $1 \leq a < 33$ und $(a, 33) = 1$ die Ordnung von a modulo 33.

(b) Es seien $a, n \in \mathbb{N}$ mit $(a, n) = 1$. Zeigen Sie: $\mathrm{ord}_n(a) = n - 1 \Rightarrow n \in \mathbb{P}$.

Aufgabe 3*

Bestimmen Sie für $m = 17$, $m = 30$ und $m = 130$ jeweils alle Lösungen der quadratischen Kongruenz $x^2 \equiv -1 \bmod m$.

(*Hinweis:* Falls m nicht prim ist, ist Korollar 3.10 nicht anwendbar. Versuchen Sie, in diesen Fällen ein äquivalentes *System* von Kongruenzen zu finden.)

Aufgabe 4*

Es seien $m_1, \dots, m_r \in \mathbb{N}$ paarweise teilerfremd und $c_1, \dots, c_r \in \mathbb{Z}$. Zeigen Sie: Setzt man $m := m_1 \cdot \ldots \cdot m_r$ und $M_i := m/m_i$ für $1 \leq i \leq r$, so ist $x := \sum_{i=1}^{r} c_i M_i^{\varphi(m_i)}$ eine Lösung des Kongruenzsystems $x \equiv c_i \bmod m_i,\ 1 \leq i \leq r$.

Aufgabe 5*

Es sei $n \in \mathbb{N}$, $n > 1$. Zeigen Sie: Ist $(10, n) = 1$, so ist die Dezimalbruchentwicklung von $1/n$ periodisch mit der Periodenlänge $\mathrm{ord}_n(10)$.

Mit einem Stern (*) versehene Aufgaben werden nicht korrigiert!

5. Stundenübung

18. November 2004

Chinesischer Restsatz: Sind $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd und $c_1, \ldots, c_r \in \mathbb{Z}$, so ist das Kongruenzsystem

$$x \equiv c_i \bmod m_i,\ 1 \leq i \leq r$$

lösbar. Die Lösung ist eindeutig mod $m_1 \cdot \ldots \cdot m_r$.

Allgemeiner gilt: Es seien $m_1, \ldots, m_r \in \mathbb{N}$, $c_1, \ldots, c_r \in \mathbb{Z}$. Das Kongruenzsystem

$$x \equiv c_i \bmod m_i,\ 1 \leq i \leq r$$

ist genau dann lösbar, wenn für alle $1 \leq i < j \leq r$ gilt: $c_i \equiv c_j \bmod \mathrm{ggT}(m_i, m_j)$. Die Lösung ist in diesem Fall eindeutig mod $\mathrm{kgV}(m_1, \ldots, m_r)$.

Aufgabe 1

Prüfen Sie, ob die folgenden Kongruenzsysteme lösbar sind und bestimmen Sie ggf. alle Lösungen:

$$\text{(a)} \begin{cases} 2x \equiv 1 \bmod 3 \\ x \equiv 3 \bmod 5 \\ 4x \equiv 2 \bmod 7 \end{cases} \qquad \text{(b)} \begin{cases} x \equiv 5 \bmod 16 \\ x \equiv 1 \bmod 20 \\ x \equiv 7 \bmod 18 \end{cases}$$

Aufgabe 2

Folgern Sie aus dem Chinesischen Restsatz: Sind $m_1, m_2, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd, so gilt für alle $x, y \in \mathbb{Z}$:

$$x \equiv y \bmod m_1 \cdot m_2 \cdot \ldots \cdot m_r \Leftrightarrow \begin{cases} x \equiv y \bmod m_1 \\ x \equiv y \bmod m_2 \\ \quad \ldots \\ x \equiv y \bmod m_r \end{cases}$$

Bestimmen Sie damit die Lösungsmenge der Kongruenz $135x \equiv 833 \bmod 1001$.

Aufgabe 3

(a) Zeigen Sie mit Hilfe des Kleinen Satzes von Fermat: $101 \mid (5^{2004} - 19)$.

(b) Bestimmen Sie mit Hilfe des Satzes von Wilson alle Lösungen der quadratischen Kongruenz $x^2 \equiv -1 \bmod 41$.

Aufgabe 4

Es seien $a, m \in \mathbb{N}$ teilerfremd, und $n := \mathrm{ord}_m(a)$ bezeichne die Ordnung von a modulo m. (Zur Erinnerung: Dies ist die kleinste natürliche Zahl n mit $a^n \equiv 1 \bmod m$.)

Zeigen Sie, daß für jedes $k \in \mathbb{N}$ gilt: $\mathrm{ord}_m(a^k) = \dfrac{n}{(k, n)}$.

Bestimmen Sie für jedes a mit $1 \leq a < 20$ und $(a, 20) = 1$ die Ordnung von a modulo 20. Berechnen Sie außerdem für $a = 4$ und $a = 5$ jeweils die Menge $\{a^k \bmod 20, k \in \mathbb{N}\}$.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

25. November 2004

Einführung in die Zahlentheorie

6. Übungsblatt

Abgabe vor der nächsten Übung

Aufgabe 1 (*9 Punkte*)

Bestimmen Sie für $n = 18$ und $n = 23$ jeweils sämtliche Primitivwurzeln mod n. Für welche $a \in \mathbb{Z}$ gilt $\mathrm{ord}_{23}(a) = 11$?

Aufgabe 2 (*11 Punkte*)

Aus Sicherheitsgründen beschließen Sie, daß jede an Sie gerichtete Nachricht künftig mit dem RSA-Verfahren verschlüsselt werden soll. Zu diesem Zweck wählen Sie den Modul $n = 2183$ (das Produkt der natürlich *viel* zu kleinen Primzahlen 59 und 37) sowie den Verschlüsselungsexponenten $s = 35$ und veröffentlichen beide Werte.

(a) Welche verschlüsselte Zahlenfolge müßten Ihnen Freunde übermitteln, die Ihnen im RSA-Code „HALLO“ sagen wollen?

(Schreiben Sie 1 für „A“, 2 für „B“, ... , 26 für „Z“, um Buchstaben durch Zahlen darzustellen.)

(b) Die erste Nachricht, die Sie erhalten, lautet:

753 1347 520 753 753 1347 520 753 753 1347 520 753

Entschlüsseln Sie diese Zahlenfolge.

Hinweis: Wiederholtes Quadrieren mod 2183 liefert

$8^2 \equiv 64$	$64^2 \equiv 1913$	$1913^2 \equiv 861$	$861^2 \equiv 1284$	$1284^2 \equiv 491$
$12^2 \equiv 144$	$144^2 \equiv 1089$	$1089^2 \equiv 552$	$552^2 \equiv 1267$	$1267^2 \equiv 784$
$15^2 \equiv 225$	$225^2 \equiv 416$	$416^2 \equiv 599$	$599^2 \equiv 789$	$789^2 \equiv 366$

$753^2 \equiv -571$	$571^2 \equiv 774$	$774^2 \equiv 934$	$934^2 \equiv -844$	$844^2 \equiv 678$	$678^2 \equiv -929$	$929^2 \equiv 756$
$1347^2 \equiv 336$	$336^2 \equiv -620$	$620^2 \equiv 192$	$192^2 \equiv -247$	$247^2 \equiv -115$	$115^2 \equiv 127$	$127^2 \equiv 848$
$520^2 \equiv -292$	$292^2 \equiv 127$	$127^2 \equiv 848$	$848^2 \equiv 897$	$897^2 \equiv -918$	$918^2 \equiv 86$	$86^2 \equiv 847$

Aufgabe 3*

Die natürliche Zahl n sei das Produkt zweier Primzahlen p und q. Bekanntlich läßt sich aus p und q leicht $\varphi(n)$ berechnen. Zeigen Sie, daß sich umgekehrt die Zerlegung $n = p \cdot q$ allein anhand der Werte von n und $\varphi(n)$ bestimmen läßt.

Aufgabe 4*

Zeigen Sie: Ist a eine Quadratzahl, so ist a nur für endlich viele $p \in \mathbb{P}$ eine Primitivwurzel mod p. (*Hinweis:* Bestimmen Sie $a^{(p-1)/2}$ mod p für ungerades $p \in \mathbb{P}$.)

Mit einem Stern (*) versehene Aufgaben werden nicht korrigiert!

6. Stundenübung

25. November 2004

Definition: Es sei $m \in \mathbb{N}$. Ein $a \in \mathbb{Z}$ mit $(a, m) = 1$ heißt *Primitivwurzel* mod m, falls $\mathrm{ord}_m(a) = \varphi(m)$ gilt.

Satz: Primitivwurzeln mod m existieren genau für folgende Moduln m:

- $m \in \{1, 2, 4\}$
- $m = p^k$ für eine ungerade Primzahl p und ein $k \in \mathbb{N}$
- $m = 2p^k$ für eine ungerade Primzahl p und ein $k \in \mathbb{N}$

Aufgabe 1

(a) Bestimmen Sie für $n = 9, 15, 31$ jeweils alle Primitivwurzeln mod n.

(b) Es sei $m > 2$, und $a \in \mathbb{Z}$ sei teilerfremd zu m. Zeigen Sie, daß a genau dann eine Primitivwurzel mod m ist, wenn für jeden echten Primteiler q von $\varphi(m)$ gilt: $a^{\varphi(m)/q} \not\equiv 1 \bmod m$.

(c) Beweisen Sie den Satz von Wilson mit Hilfe von Primitivwurzeln.

Aufgabe 2

Es sei $n = p \cdot q$ mit $p, q \in \mathbb{P}$, außerdem sei ein festes $s \in \mathbb{N}$ mit $(s, \phi(n)) = 1$ gewählt. Wir „verschlüsseln“ nun jede zu n teilerfremde Zahl $X \in \{1, 2, \ldots, n-1\}$, indem wir $\tilde{X} \in \{1, 2, \ldots, n-1\}$ mit $\tilde{X} \equiv X^s \bmod n$ berechnen.
Die Zuordnung $X \mapsto \tilde{X}$ nennt man *RSA-Code* zum *Verschlüsselungsexponenten* s und Modul n (RSA = Rivest, Shamir und Adleman).

(a) Es sei $\tilde{X}$ die RSA-Codierung von X wie oben beschreiben. Zeigen Sie, wie sich X aus $\tilde{X}$ zurückgewinnen läßt, wenn man ein $t \in \mathbb{N}$ mit $s \cdot t \equiv 1 \bmod \phi(n)$ kennt.

(Die Voraussetzung $(s, \phi(n)) = 1$ garantiert, daß es ein solches t gibt!)

(b) Verschlüsseln Sie die Zahl $X = 10$ mit dem RSA-Code zu $n = 391$ und $s = 7$.

(c) Eine geheime Zahl X ist mit demselben Code wie in (b) zu $\tilde{X} = 20$ verschlüsselt worden. Bestimmen Sie X.

Zum Verschlüsseln benötigt man offenbar nur n und s; um einen Entschlüsselungsexponenten t wie in (a) zu bestimmen, muß man hingegen $\phi(n)$ kennen. Wenn nun p und q groß genug gewählt sind (sagen wir: mehrere hundert Stellen jeweils), ist die Chance verschwindend, allein anhand von n die Zerlegung $n = p \cdot q$ zu finden, mit der man $\phi(n)$ einfach ausrechnen könnte. In diesem Fall kann man also n und s getrost veröffentlichen und so von beliebigen Absendern codierte Nachrichten empfangen, die niemand außer einem selbst wieder decodieren kann! (Ein solches Verschlüsselungsverfahren heißt *public key code*.)

Hinweis: Wiederholtes Quadrieren mod 391 liefert

$20^2 \equiv 9$ $\quad 20^4 \equiv 9^2 \equiv 81$ $\quad 20^8 \equiv 81^2 \equiv 305$ $\quad 20^{16} \equiv 305^2 \equiv 358$
$20^{32} \equiv 358^2 \equiv 307$ $\quad 20^{64} \equiv 307^2 \equiv 18$ $\quad 20^{128} \equiv 18^2 \equiv 324$

Außerdem ist $324 \cdot 358 \cdot 81 \cdot 9 \cdot 20 \equiv 385 \bmod 391$.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

2. Dezember 2004

Einführung in die Zahlentheorie

7. Übungsblatt

Abgabe vor der nächsten Übung

Aufgabe 1 (*6 Punkte*)

Bestimmen Sie jeweils alle quadratischen Reste mod 16 bzw. mod 23. Geben Sie drei Primzahlen p mit $67 < p < 131$ an, für die 2 ein quadratischer Rest mod p, aber -1 kein quadratischer Rest mod p ist.

Aufgabe 2 (*8 Punkte*)

$p := 313$ und $q := 613$ sind Primzahlen. Berechnen Sie die folgenden LEGENDREsymbole:

$\left(\frac{-1}{p}\right), \left(\frac{-1}{q}\right), \left(\frac{2}{p}\right), \left(\frac{2}{q}\right), \left(\frac{q}{p}\right)$. Ist die Kongruenz $x^2 \equiv -13 \bmod 313$ lösbar?

Aufgabe 3 (*6 Punkte*)

Untersuchen Sie jede der folgenden Kongruenzen auf Lösbarkeit und bestimmen Sie gegebenenfalls alle Lösungen:

$15x^2 + 8x + 5 \equiv 0 \bmod 13 \quad , \quad 10x^2 + x + 10 \equiv 0 \bmod 19 \quad , \quad 12x^2 + 11x + 35 \equiv 0 \bmod 59$

Aufgabe 4*

Sei $p \in \mathbb{P}$ und $M_p := 2^p - 1$. Beweisen Sie: Ist p eine ungerade Primzahl und q ein Primteiler von M_p, so gilt $q \equiv 1 \bmod 2p$ und $q \equiv \pm 1 \bmod 8$. Benutzen Sie diese Aussage, um mit möglichst geringem Rechenaufwand zu zeigen, daß $M_{17} = 2^{17} - 1 = 131071$ eine Primzahl ist.

Hinweis: Von den Zahlen $q = 2 \cdot k \cdot 17 + 1$ mit $q^2 \leq M_{17}$ sind nur die folgenden prim: 103, 137, 239, 307.

Mit einem Stern (*) versehene Aufgaben werden nicht korrigiert!

7. Stundenübung

2. Dezember 2004

Quadratische Reziprozität: $p, q \in \mathbb{P}_{>2}, p \neq q \Rightarrow \left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right), & \text{falls } p \equiv q \equiv 3 \bmod 4 \\ \left(\frac{q}{p}\right) & \text{sonst} \end{cases}$

Ergänzungsgesetze: $p \in \mathbb{P}_{>2} \Rightarrow \left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv 1 \bmod 4 \\ -1, & \text{falls } p \equiv 3 \bmod 4 \end{cases}$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv \pm 1 \bmod 8 \\ -1, & \text{falls } p \equiv \pm 3 \bmod 8 \end{cases}$$

Aufgabe 1

Bestimmen Sie jeweils alle quadratischen Reste mod 12 bzw. mod 19.
Geben Sie drei Primzahlen p mit $23 < p < 59$ an, für die -1 quadratischer Rest mod p, aber 2 kein quadratischer Rest mod p ist.

Aufgabe 2

$p := 439$ und $q := 197$ sind Primzahlen. Berechnen Sie folgende LEGENDREsymbole:
$\left(\frac{-1}{p}\right), \left(\frac{-1}{q}\right), \left(\frac{2}{p}\right), \left(\frac{2}{q}\right), \left(\frac{q}{p}\right)$.
Ist die Kongruenz $x^2 \equiv 197 \bmod 439$ lösbar?

Aufgabe 3

Es sei p eine ungerade Primzahl und a eine zu p teilerfremde ganze Zahl. Beweisen Sie: Die Kongruenz

$$ax^2 + bx + c \equiv 0 \bmod p$$

ist dann und nur dann lösbar, wenn ihre *Diskriminante* $D := b^2 - 4ac$ kein quadratischer Nichtrest mod p ist (d. h. wenn $\left(\frac{D}{p}\right) = 0$ oder 1 ist).

Aufgabe 4

Untersuchen Sie jede der folgenden Kongruenzen auf Lösbarkeit und bestimmen Sie gegebenenfalls alle Lösungen.

$$2x^2 - x + 3 \equiv 0 \bmod 5 \quad , \quad 5x^2 + 2x + 3 \equiv 0 \bmod 7$$

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

9. Dezember 2004

Einführung in die Zahlentheorie

8. Übungsblatt

Abgabe vor der nächsten Übung

Aufgabe 1 (*8 Punkte*)

(a) Berechnen Sie die Jacobi-Symbole $\left(\frac{7}{143}\right)$, $\left(\frac{39}{35}\right)$ und $\left(\frac{499}{1001}\right)$.

(b) Untersuchen Sie, welche der folgenden Kongruenzen lösbar sind, und bestimmen Sie ggf. alle Lösungen: $x^2 \equiv 7 \bmod 143$, $x^2 \equiv 39 \bmod 35$, $x^2 \equiv 499 \bmod 1001$. (Hinweis: $1001 = 7 \cdot 11 \cdot 13$)

Aufgabe 2 (*12 Punkte*)

Untersuchen Sie, welche der folgenden positiv definiten quadratischen Formen zueinander äquivalent sind:

$f_1(x,y) = 3x^2 + 11xy + 15y^2$
$f_2(x,y) = 35x^2 + 121xy + 105y^2$
$f_3(x,y) = 3x^2 + 7xy + 9y^2$
$f_4(x,y) = 3x^2 + 5xy + 7y^2$

Bestimmen Sie zu jeder dieser quadratischen Formen die zugehörige reduzierte Form und geben Sie jeweils eine unimodulare Matrix T an, die die Matrix F der quadratischen Form $f(x,y) = \vec{x}^{\,t} F \vec{x}$ in die Matrix G der zugehörigen reduzierten Form $g(x,y) = \vec{x}^{\,t} G \vec{x}$ überführt (d. h. $G = T^t F T$).

Aufgabe 3*

(a) Bestimmen Sie alle reduzierten positiv definiten quadratischen Formen f mit Diskriminante $d_f \geq -15$ und berechnen Sie damit die Klassenzahl $h(d)$ für $-15 \leq d < 0$.

(b) Bestimmen Sie die Klassenzahl $h(-163)$.

(c) Es sei $d < 0$ mit $d \equiv 0$ oder $1 \bmod 4$. Zeigen Sie: $h(d) > 0$.

Mit einem Stern (*) versehene Aufgaben werden nicht korrigiert!

8. Stundenübung

9. Dezember 2004

Quadratische Form: $f(x,y) = ax^2 + bxy + cy^2 = \vec{x}^{\,t} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \vec{x}\,; \qquad a,b,c \in \mathbb{Z},\ \vec{x} = \begin{pmatrix} x \\ y \end{pmatrix}.$

$d_f := b^2 - 4ac$ heißt *Diskriminante* von f. Ist $d_f < 0$ und $a \geq 0$, so heißt f *positiv definit*. Eine positiv definite Form f heißt *reduziert*, falls gilt: $-a < b \leq a < c$ oder $0 \leq b \leq a = c$.

Eine (2×2)–Matrix T mit ganzzahligen Einträgen und $\det T = 1$ heißt *unimodular*; die zugehörige Variablensubstitution $\vec{x} \mapsto T\,\vec{x}$ ist dann eine Bijektion von $\mathbb{Z} \times \mathbb{Z}$ auf $\mathbb{Z} \times \mathbb{Z}$.

Zwei quadratische Formen $f(\vec{x}) = \vec{x}^{\,t} F\,\vec{x}$ und $g(\vec{x}) = \vec{x}^{\,t} G\,\vec{x}$ heißen *äquivalent*, falls es eine unimodulare Matrix T gibt, so daß $g(\vec{x}) = f(T\,\vec{x})$ bzw. $G = T^t F T$ gilt. Zueinander äquivalente Formen haben dieselbe Diskriminante und dieselbe Wertemenge.

Nützliche unimodulare Matrizen: $T_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ T_\pm = \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}.$

Ist $f(\vec{x}) = ax^2 + bxy + cy^2$, so ist $f(T_0\,\vec{x}) = cx^2 - bxy + ay^2$,
$f(T_+\,\vec{x}) = ax^2 + (b+2a)xy + (a+b+c)y^2$ und
$f(T_-\,\vec{x}) = ax^2 + (b-2a)xy + (a-b+c)y^2$.

Mit Hilfe dieser Transformationen läßt sich jede positiv definite Form f in eine äquivalente reduzierte Form überführen. Zwei quadratische Formen sind genau dann äquivalent, wenn die zugehörigen reduzierten Formen übereinstimmen.

Aufgabe 1

(a) Berechnen Sie die Jacobi-Symbole $\left(\frac{7}{9}\right)$, $\left(\frac{7}{323}\right)$ und $\left(\frac{7}{391}\right)$.

(b) Untersuchen Sie, welche der folgenden Kongruenzen lösbar sind, und bestimmen Sie ggf. alle Lösungen: $x^2 \equiv 7 \bmod 9$, $x^2 \equiv 7 \bmod 323$, $x^2 \equiv 7 \bmod 391$.

Aufgabe 2

Untersuchen Sie, welche der folgenden positiv definiten quadratischen Formen zueinander äquivalent sind:

$f_1(x,y) = 2x^2 - xy + 5y^2$, $\quad f_2(x,y) = 6x^2 + 21xy + 20y^2$,
$f_3(x,y) = 13x^2 + 13xy + 4y^2$, $\quad f_4(x,y) = 2x^2 + 2xy + 5y^2$.

Bestimmen Sie zu jeder dieser quadratischen Formen die zugehörige reduzierte Form. Geben Sie in jedem Fall eine unimodulare Matrix T an, die die Matrix F der quadratischen Form $f(x,y) = \vec{x}^{\,t} F\,\vec{x}$ in die Matrix G der zugehörigen reduzierten Form $g(x,y) = \vec{x}^{\,t} G\,\vec{x}$ überführt (d. h. $G = T^t F T$).

Aufgabe 3

Berechnen Sie für $-18 \leq d \leq -16$ jeweils die Klassenzahl $h(d)$, indem sie alle reduzierten positiv definiten quadratischen Formen $f(x,y) = ax^2 + bxy + cy^2$ mit der Diskriminante d bestimmen.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

16. Dezember 2004

Einführung in die Zahlentheorie

9. Übungsblatt

Abgabe vor der nächsten Übung

Aufgabe 1 (*6+2+2 Punkte*)

(a) Stellen Sie mit Hilfe der Methode des Abstiegs die Primzahlen 809 und 1553 als Summe zweier Quadrate dar. (Hinweis: $318^2 \equiv -1 \bmod 809$, $339^2 \equiv -1 \bmod 1553$)

(b) Stellen Sie $8177 = 13 \cdot 17 \cdot 37$ auf vier verschiedene Weisen als Summe zweier Quadrate dar, d. h. bestimmen Sie vier verschiedene Paare (x, y) mit $x, y \in \mathbb{N}$, $x \leq y$ und $x^2 + y^2 = 8177$.

(c) Stellen Sie 8177 als Summe von vier positiven Quadraten dar, d. h. bestimmen Sie $u, v, w, x \in \mathbb{N}$ mit $u^2 + v^2 + w^2 + x^2 = 8177$.

Aufgabe 2 (*7 Punkte*)

Bestimmen Sie alle ganzzahligen Lösungen der Gleichung $9x^2 + 26xy + 19y^2 = 187$.

Aufgabe 3 (*3 Punkte*)

Es sei $n \in \mathbb{N}$ mit $n \equiv 7 \bmod 8$. Zeigen Sie, daß sich n nicht als Summe von drei Quadraten darstellen läßt.

Aufgabe 4* (*etwas zum Nachdenken für die vorlesungsfreie Zeit*)

Ich wähle zwei natürliche Zahlen a und b, beide ≥ 2. Dem Mathematiker S verrate ich die Summe $a + b$, seiner Kollegin P das Produkt ab. Beide kennen also nur ihr eigenes Ergebnis (und die eingangs erwähnten Voraussetzungen über a und b), nicht aber die Zahlen a und b selbst. Ich stelle sowohl P als auch S nun die Aufgabe, das Ergebnis des jeweils anderen herauszufinden. Daraufhin spielt sich folgendes Telefongespräch ab:

S: Hallo, hier spricht S. Nehmen Sie's nicht persönlich, aber ich sehe keinen Weg, wie Sie meine Summe bestimmen können.
P: Danke für die Information. Ich kenne jetzt Ihre Summe.
S: Jetzt kenne ich auch Ihr Produkt.

Welche Zahlen habe ich mir ausgedacht? Ich verrate Ihnen zusätzlich, daß beide ≤ 20 sind.

Wäre die Lösung immer noch sinnvoll, wenn ich auch P und S von vornherein mitgeteilt hätte, daß $a, b \leq 20$ gilt?

Klausurtermin: Dienstag, 25.Januar 2005, 10:00 in F128.

Frohe Weihnachten und ein glückliches neues Jahr!

9. Stundenübung

16. Dezember 2004

Methode des Abstiegs für die Summe von zwei Quadraten: Es sei $p \in \mathbb{P}$, $p \equiv 1 \bmod 4$. Kennt man eine Darstellung von hp $(0 < h < p)$ als Summe von zwei Quadraten, kann man folgende Konstruktion durchführen:

$x^2 + y^2 = hp \;\rightarrow$ bestimme betragskleinste Reste $u \equiv x \bmod h$, $v \equiv y \bmod h$;
def. $x' := \dfrac{xu + yv}{h}, y' := \dfrac{xv - yu}{h}$. Dann ist $(x')^2 + (y')^2 = h'p$ mit $h' < h$.

Einige nützliche Identitäten:

$$(1) \qquad \begin{aligned}(x^2+y^2)(u^2+v^2) &= (xu+yv)^2 + (xv-yu)^2 \\ &= (xu-yv)^2 + (xv+yu)^2\end{aligned}$$

$$(2) \qquad \begin{aligned}(x^2+ay^2)(u^2+av^2) &= (xu+ayv)^2 + a(xv-yu)^2 \\ &= (xu-ayv)^2 + a(xv+yu)^2\end{aligned}$$

$$(3) \qquad (x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = z_1^2+z_2^2+z_3^2+z_4^2$$

mit
$$z_1 := x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \qquad z_2 := x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3$$
$$z_3 := x_1y_3 + x_2y_4 - x_3y_1 - x_4y_2, \qquad z_4 := x_1y_4 - x_2y_3 + x_3y_2 - x_4y_1$$

Aufgabe 1

Fermats Methode des Abstiegs läßt sich in allgemeiner Form wie folgt beschreiben:

Es sei M eine nichtleere Menge natürlicher Zahlen mit der Eigenschaft, daß zu jedem $h \in M$, $h > 1$, ein $h' \in M$, $h' < h$, existiert. Dann ist $1 \in M$.

(a) Es sei $p \in \mathbb{P}$ mit $p \equiv 1 \bmod 4$. Zeigen Sie mit der Methode des Abstiegs, daß sich p als Summe zweier Quadrate darstellen läßt.

(Hinweis: Betrachten Sie die Menge M aller $h \in \{1, 2, \ldots, p-1\}$, für die sich hp als Summe zweier Quadrate darstellen läßt.)

(b) Konstruieren Sie mit der Methode des Abstiegs eine Darstellung der Primzahl 277 als Summe zweier Quadrate.

Aufgabe 2

Stellen Sie $1189 = 29 \cdot 41$ auf zwei verschiedene Weisen als Summe zweier Quadrate dar, d. h. bestimmen Sie zwei verschiedene Paare (x, y) mit $x, y \in \mathbb{N}$, $x \leq y$ und $x^2 + y^2 = 1189$.

Aufgabe 3

Bestimmen Sie alle ganzzahligen Lösungen der Gleichung $3x^2 + 12xy + 13y^2 = 91$. (Hinweis: Finden Sie die zu $3x^2 + 12xy + 13y^2$ äquivalente reduzierte Form.)

Aufgabe 4

Stellen Sie 3003 als Summe von vier Quadraten dar.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

13. Januar 2005

Einführung in die Zahlentheorie

10. Übungsblatt

Abgabe vor der nächsten Übung

Aufgabe 1 (*6 Punkte*)

Zeigen Sie, daß eine Konstante $K > 0$ existiert mit folgender Eigenschaft: Für $x \geq 2$ gibt es stets eine Primzahl p mit $x < p \leq K \cdot x$. (*Hinweis:* Zeigen Sie mit dem Satz von Mertens, daß es ein $K > 0$ gibt mit $\displaystyle\sum_{x<p\leq Kx} \frac{\log p}{p} > 0$ für alle $x \geq 2$.)

Aufgabe 2 (*6+4+4 Punkte*)

(a) Stellen Sie $\alpha = 1051/621$ als normierten Kettenbruch $\alpha = \langle a_0; a_1, \ldots, a_n\rangle$, $a_n \neq 1$, dar und bestimmen Sie sämtliche Näherungsbrüche zu α.

(b) Es sei $\alpha := 1.27354621$. Bestimmen Sie die bestmögliche rationale Approximation p/q für α, deren Nenner $q < 100$ ist. Geben Sie außerdem einen Näherungsbruch p/q für α an mit $|\alpha - p/q| < 5 \cdot 10^{-5}$.

(c) Es sei $\alpha = \langle a_0; a_1, a_2, \ldots\rangle$ ein (endlicher oder unendlicher) Kettenbruch. Wie lauten die Kettenbruchdarstellungen der Zahlen $1 + \alpha$, $\{\alpha\}$ und $1/\alpha$?

Aufgabe 3*

(a) Die Kettenbruchdarstellung von π lautet $\langle 3; 7, 15, 1, 292, 1, 1, \ldots\rangle$. Bestimmen Sie jeweils die bestmögliche rationale Näherung $\pi \approx p/q$ mit $q < 10$ bzw. $q < 10000$.

(b) Ein recht genauer Wert für die Umlaufzeit der Erde um die Sonne ist $365 + \alpha$ Tage, wobei $\alpha = 104629/432000$. Approximieren Sie α möglichst gut durch einen Bruch p/q mit Nenner $q < 1000$.

(c) Bestimmen Sie mit Hilfe eines Taschenrechners den Beginn der Kettenbruchentwicklung von π^4 und vergleichen Sie ihre Ergebnisse mit dem wahren Wert

$$\pi^4 = \langle 97; 2, 2, 3, 1, 16539, 1, \ldots\rangle$$

(d) Bestimmen Sie für $\alpha = \pi^4$ die beste rationale Approximation p/q, deren Nenner $q < 10^5$ ist, und geben Sie eine obere Schranke für den Fehler $|\alpha - p/q|$ an.

Mit einem Stern (*) versehene Aufgaben werden nicht korrigiert!

10. Stundenübung

13. Januar 2005

Abelsche Teilsummation: Es sei $(\lambda_n)_{n\in\mathbb{N}}$ eine streng monoton gegen ∞ wachsende Folge; weiter sei $(a_n)_{n\in\mathbb{N}}$ eine beliebige Folge reeller Zahlen und f eine stetig differenzierbare Funktion, so daß $f(t)$ für alle $t \geq \lambda_1$ definiert ist. Dann gilt mit $A(x) := \sum_{\lambda_n \leq x} a_n$:

$$\sum_{\lambda_n \leq x} a_n f(\lambda_n) = A(x)f(x) - \int_{\lambda_1}^{x} A(t)f'(t)dt$$

Satz von Mertens: $\displaystyle\sum_{p\leq x,\, p\in\mathbb{P}} \frac{\log p}{p} = \log x + O(1) \quad \text{für } x \geq 2$

$\alpha = \langle a_0; a_1, a_2, \dots \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots}}}$ sei ein (endlicher oder unendlicher) Kettenbruch.

Dann läßt sich der *n-te Näherungsbruch* $\langle a_0; a_1, \dots, a_n \rangle = p_n/q_n$ mit Hilfe der folgenden Rekursionsformeln berechnen:

$$\begin{array}{llll} p_{-1} = 1, & p_0 = a_0, & p_k = a_k p_{k-1} + p_{k-2} & (k \geq 2) \\ q_{-1} = 0, & q_0 = 1, & q_k = a_k q_{k-1} + q_{k-2} & (k \geq 2) \end{array}$$

Der n-te Näherungsbruch ist die bestmögliche rationale Approximation für α mit Nenner $< q_{n+1}$.

Aufgabe 1

Beweisen Sie mit Teilsummation und dem Satz von Mertens, daß für $x \geq 2$ gilt:

$$\sum_{p\leq x,\, p\in\mathbb{P}} \frac{(\log p)^2}{p} = \frac{1}{2}(\log x)^2 + O(\log x)$$

Aufgabe 2

Stellen Sie $\alpha = 180/79$ als normierten Kettenbruch $\alpha = \langle a_0; a_1, a_2, \dots, a_n \rangle$, $a_n \neq 1$, dar und bestimmen Sie die Näherungsbrüche $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \dots, \frac{p_n}{q_n} = \alpha$. Verifizieren Sie die Fehlerabschätzung $|\alpha - \frac{p_k}{q_k}| \leq \frac{1}{q_k q_{k+1}} \leq \frac{1}{q_k^2}$ für $k = 0, 1, \dots n-1$.

Aufgabe 3

Für $x \in \mathbb{R}$ bezeichne $\{x\} := x - [x]$ den Bruchteil von x.

(a) Es sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ gegeben, und die Folge $(\vartheta_n)_{n\in\mathbb{N}}$ sei rekursiv definiert durch $\vartheta_0 := \alpha$ und $\vartheta_{n+1} = \frac{1}{\{\vartheta_n\}}$. Zeigen Sie: $\alpha = \langle\, [\vartheta_0]\,;\, [\vartheta_1], [\vartheta_2], \dots \rangle$

(b) Bestimmen Sie mit Hilfe eines Taschenrechners den Beginn der Kettenbruchentwicklung von $\alpha := 0.12345556$ und geben Sie die bestmögliche rationale Näherung für α an, deren Nenner ≤ 10000 ist.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

20. Januar 2005

Einführung in die Zahlentheorie

11. Übungsblatt

Aufgabe 1*

(a) Bestimmen Sie die Kettenbrüche von $\sqrt{3}$, $\sqrt{5}$ und $\sqrt{a^2+2a}$ für $a \in \mathbb{N}$.

(b) Bestimmen Sie den periodischen Kettenbruch von $(11-\sqrt{14})/4$ mit Hilfe eines Taschenrechners und der Information, daß Vorperiode und Periode höchstens die Länge 4 haben.

(c) Bestimmen Sie zu $\alpha = \langle\, \overline{2}\,\rangle$ und $\alpha = \langle\, 1; 2, \overline{1,2,1}\,\rangle$ jeweils ein quadratisches Polynom $f(x)$ mit ganzzahligen Koeffizienten, so daß $f(\alpha) = 0$ ist.

Aufgabe 2*

Von der reellen Zahl α sei nur bekannt, daß $\left|\alpha - \frac{98}{67}\right| < 0.0001$ ist. Bestimmen Sie den Anfang der Kettenbruchentwicklung von α.

Aufgabe 3*

Die Folge $(F_n)_{n\in\mathbb{N}}$ der *Fibonacci-Zahlen* ist rekursiv definiert durch $F_1 := 1$, $F_2 := 1$ und $F_n = F_{n-1} + F_{n-2}$ für $n > 2$.

(a) Berechnen Sie $F_1, F_2, \ldots, F_{16}$.

(b) Stellen Sie für $n \in \mathbb{N}$ die rationale Zahl F_{n+1}/F_n als Kettenbruch dar. (Hinweis: Betrachten Sie einige Beispiele und beweisen Sie die sich aufdrängende Vermutung.)

(c) Zeigen Sie, daß das Verhältnis F_{n+1}/F_n aufeinanderfolgender Fibonacci-Zahlen für $n \to \infty$ gegen den goldenen Schnitt $(1+\sqrt{5})/2$ konvergiert.

Mit einem Stern (*) versehene Aufgaben werden nicht korrigiert!

Klausur: Di, 25.01.05, 10:00 in F128. Als Hilfsmittel sind zugelassen: Taschenrechner (nicht programmierbar) sowie ein eigenhändig beschriebenes DIN-A4-Blatt (keine Ausdrucke oder Kopien).

11. Stundenübung

20. Januar 2005

Eine reelle Zahl α heißt *quadratisch irrational*, falls $\alpha \notin \mathbb{Q}$ gilt und α Nullstelle eines quadratischen Polynoms $f(x)$ mit ganzzahligen Koeffizienten ist. Jede quadratisch irrationale Zahl läßt sich auf die Form $\alpha = (a + \sqrt{b})/c$ mit $a, b, c \in \mathbb{Z}$ bringen.

Ein Satz von Lagrange besagt, daß $\alpha \in \mathbb{R}$ genau dann quadratisch irrational ist, wenn α eine (rein- oder gemischt-)periodische Kettenbruchdarstellung besitzt.

—

Allgemeiner heißt $\alpha \in \mathbb{R}$ *algebraisch vom Grad n*, falls es ein Polynom n-ten Grades $f(x) \in \mathbb{Z}[x]$ mit $f(\alpha) = 0$ gibt und außer dem Nullpolynom kein Polynom kleineren Grades mit dieser Eigenschaft existiert. Reelle Zahlen, die nicht algebraisch von irgendeinem Grad sind, heißen *transzendent*.

Satz von Liouville: α sei algebraisch vom Grad $n \geq 2$. Dann existiert ein $c > 0$, so daß für alle $\frac{p}{q} \in \mathbb{Q}$ mit $q > 0$ gilt: $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}$.

Aufgabe 1

(a) Bestimmen Sie die Kettenbrüche von $\sqrt{2}$ und $6 - \sqrt{7}$.

(b) Bestimmen Sie zu den periodischen Kettenbrüchen $\alpha = \langle\, \overline{1} \,\rangle := \langle 1; 1, 1, 1, \ldots \rangle$ und $\alpha = \langle\, 1; 5, \overline{2, 3} \,\rangle := \langle\, 1; 5, 2, 3, 2, 3, 2, 3, \ldots \,\rangle$ jeweils ein quadratisches Polynom $f(x)$ mit ganzzahligen Koeffizienten, so daß $f(\alpha) = 0$ ist.

(c) Es sei $a \in \mathbb{N}$. Wie lautet der Kettenbruch zu $\sqrt{a^2 + 1}$?

Aufgabe 2

(a) Über die reelle Zahl α sei nur bekannt, daß $\left|\alpha - \frac{73}{49}\right| < 0.0002$ ist. Bestimmen Sie den Anfang der Kettenbruchentwicklung von α.

(b) Genau einer der Brüche $\frac{62}{49}, \frac{6}{5}, \frac{29}{23}, \frac{285}{227}$ ist ein Näherungsbruch von $\sqrt[3]{2}$. Finden Sie heraus, welcher es ist, ohne den Kettenbruch von $\sqrt[3]{2}$ explizit zu berechnen.

Aufgabe 3

Zeigen Sie, daß die reelle Zahl $\alpha := \sum_{k=0}^{\infty} 10^{-3^k} = 0.10100000100000000000000001000\ldots$ nicht algebraisch vom Grad ≤ 2 ist.