INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

21. Oktober 2004

Einführung in die Zahlentheorie

Lösungshinweise zum 1. Übungsblatt

Aufgabe 1

a) läßt sich mit Induktion über n zeigen. Im Falle $n = 1$ erhält man die wahre Aussage $15 \mid 15$, und für den Induktionsschritt „$n \to n+1$“ betrachtet man

$$2^{4(n+1)} - 1 = 16 \cdot 2^{4n} - 1 = 15 \cdot 2^{4n} + (2^{4n} - 1)$$

Der erste Summand ist stets durch 15 teilbar; setzt man also voraus, daß $15 \mid 2^{4n} - 1$ für ein $n \in \mathbb{N}$ gilt, folgt automatisch $15 \mid 2^{4(n+1)} - 1$.

b) $N := (n^2+3n)(n^2-1)(n^2-4) = (n-2)(n-1)n(n+1)(n+2)(n+3)$ ist das Produkt von sechs aufeinanderfolgenden ganzen Zahlen.

Unter diesen Zahlen sind in jedem Fall drei gerade, und mindestens eine von diesen dreien ist sogar durch 4 teilbar, also ist N sicher durch 16 teilbar. (N ist von der Form $2k \cdot 2l \cdot 4m \cdot \ldots$ mit $k, l, m \in \mathbb{Z}$.) Außerdem müssen zwei der sechs Faktoren durch 3 (N also durch 9) und einer durch 5 teilbar sein.

Diese Bestandsaufnahme zeigt, daß N durch 16, 9 und 5 teilbar ist und damit auch durch $16 \cdot 9 \cdot 5 = 720$. (Da 16, 9 und 5 paarweise teilerfremd sind, ist dieser Schluß immer erlaubt; hier muß man sich nicht mehr überlegen, ob die Teiler in unterschiedlichen Faktoren „sitzen“ oder nicht.)

Aufgabe 2

Euklid liefert

$$\begin{aligned} 8091 &= 1 \cdot 5425 + 2666 \\ 5425 &= 2 \cdot 2666 + 93 \\ 2666 &= 28 \cdot 93 + 62 \\ 93 &= 1 \cdot 62 + 31 \\ 62 &= 2 \cdot 31 \end{aligned}$$

Der letzte Rest, bevor die Division aufgeht, ist 31 $\Rightarrow \mathrm{ggT}(8091, 5425) = 31$.

Eine Darstellung $31 = ax + by$ mit $x, y \in \mathbb{Z}$ erhält man z. B. durch Zurückrechnen von unten nach oben (vgl. Vorlesung) oder nach folgendem Schema (das man natürlich auch gleichzeitig mit dem Euklidischen Algorithmus durchrechnen kann):

$$\begin{aligned} 8091 &= 1 \cdot a + 0 \cdot b \\ 5425 &= 0 \cdot a + 1 \cdot b && \text{1-mal von der Gleichung darüber subtrahieren:} \\ 2666 &= 1 \cdot a - 1 \cdot b && \text{2-mal von der Gleichung darüber subtrahieren:} \\ 93 &= -2 \cdot a + 3 \cdot b && \text{28-mal von der Gleichung darüber subtrahieren:} \\ 62 &= 57 \cdot a - 85 \cdot b && \text{1-mal von der Gleichung darüber subtrahieren:} \\ 31 &= -59 \cdot a + 88 \cdot b \end{aligned}$$

Probe: $-59 \cdot a + 88 \cdot b = -59 \cdot 8091 + 88 \cdot 5425 = 31 \quad \checkmark$

Die Zahlen c, die sich als ganzzahlige Linearkombination $ax + by$ darstellen lassen, sind genau die ganzzahligen Vielfachen von $\mathrm{ggT}(a, b)$. Aus $31 \nmid 99$ folgt also, daß die diophantische Gleichung $ax + by = 99$ *keine* Lösung besitzt.

Für die diophantische Gleichung $ax + by = 341$ gewinnen wir jedoch wegen $341 = 11 \cdot 31$ leicht eine spezielle Lösung (x_0, y_0) aus der oben gefunden Darstellung:

$$\begin{array}{rrcll} & -59 \cdot a + 88 \cdot b & = & 31 & \mid \cdot 11 \\ \Leftrightarrow & -649 \cdot a + 968 \cdot b & = & 341 & \end{array}$$

Eine spezielle Lösung ist demnach $(x_0, y_0) = (-649, 968)$; die allgemeine Lösung der diophantischen Gleichung $ax + by = 341$ ist (vgl. Satz 1.11):

$$(x, y) = \left(x_0 - \frac{b}{(a,b)} \cdot t,\ y_0 + \frac{a}{(a,b)} \cdot t \right) = (-649 - 175 \cdot t,\ 968 + 261 \cdot t),\ t \in \mathbb{Z}$$

Anmerkung: Für $t = -4$ erhält man die einfachere spezielle Lösung $(x_0, y_0) = (51, -76)$. Unser Verfahren liefert also i. a. keine „minimale“ Darstellung $ax_0 + by_0 = c$.

Aufgabe 3

$(a+b, a-b)$ ist gemeinsamer Teiler von $a+b$ und $a-b$, also auch von $(a+b)+(a-b) = 2a$ und $(a+b)-(a-b) = 2b$. Sind a und b teilerfremd, folgt:

$$(a + b, a - b) \mid (2a, 2b) = 2(a, b) = 2$$

Aufgabe 4

Um das Kriterium etwas mathematischer zu formulieren, schreibt man $n = 10a + b$ mit $0 \leq b < 10$ (Division mit Rest durch 10, b sind die „Einer“ in der Dezimaldarstellung von n). „Streichen der Einerstelle“ liefert dann gerade a, und das Kriterium behauptet: $7 \mid (10a + b) \Leftrightarrow 7 \mid (a - 2b)$. In dieser Form ist das aber leicht einzusehen, denn:

$$10a + b = 10(a - 2b) + 21b = 7(a - 2b) + 7 \cdot 3b + 3(a - 2b)$$

Gilt nun $7 \mid (a - 2b)$, ist jeder Summand auf der rechten Seite durch 7 teilbar und damit auch die Summe $10a + b$. Ist andererseits $10a + b$ durch 7 teilbar, so auch $3(a - 2b)$ (die beiden Terme unterscheiden sich nur um Vielfache von 7). Das geht wiederum nur, wenn bereits $a - 2b$ durch 7 teilbar ist (vgl. Hilfssatz 1.10), und beide Richtungen sind gezeigt.

Beispiel für die Anwendung:

$$7 \mid \underbrace{33\ldots33}_{k\ 3\text{en}}1 \Leftrightarrow 7 \mid \underbrace{33\ldots33}_{k\ 3\text{en}} - 2 = \underbrace{33\ldots33}_{(k-1)\ 3\text{en}}1$$

Folglich gilt: $7 \mid 31 \Leftrightarrow 7 \mid 331 \Leftrightarrow 7 \mid 3331 \Leftrightarrow \ldots$ – Keine Zahl dieser Form ist durch 7 teilbar!

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER
Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

28. Oktober 2004

Einführung in die Zahlentheorie

Lösungshinweise zum 2. Übungsblatt

Aufgabe 1

Die Primfaktorzerlegungen lauten:

$$\begin{aligned} a &= 2^3 \cdot 3 \cdot 5 \cdot 7^2 \\ b &= 2 \cdot 3^3 \cdot 7 \cdot 11 \\ (a,b) &= 2 \cdot 3 \cdot 7 \\ [a,b] &= 2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11 \end{aligned}$$

Hiermit berechnet man:

$$\begin{aligned} \varphi(a) &= \varphi(2^3) \cdot \varphi(3) \cdot \varphi(5) \cdot \varphi(7^2) \\ &= (2^3 - 2^2) \cdot (3-1) \cdot (5-1) \cdot (7^2 - 7) = 4 \cdot 2 \cdot 4 \cdot 42 = 1344 \\ \varphi(b) &= \varphi(2) \cdot \varphi(3^3) \cdot \varphi(7) \cdot \varphi(11) \\ &= (2-1) \cdot (3^3 - 3^2) \cdot (7-1) \cdot (11-1) = 1 \cdot 18 \cdot 6 \cdot 10 = 1080 \\ \varphi\left((a,b)\right) &= \varphi(2) \cdot \varphi(3) \cdot \varphi(7) = 1 \cdot 2 \cdot 6 = 12 \end{aligned}$$

Schließlich ist $\mu(a) = \mu(b) = 0$ (beide enthalten einen mehrfachen Primfaktor!) und $\mu\left((a,b)\right) = \mu(2 \cdot 3 \cdot 7) = (-1)^3 = -1$.

Aufgabe 2

Beweis: Es sei $n \in \mathbb{N}$, $n > 1$. Ist n prim, so ist keine Primzahl $p \leq \sqrt{n}$ ein Teiler von n, denn n besitzt nur die Teiler 1 (keine Primzahl) und n (Primzahl, aber $> \sqrt{n}$).
Ist andererseits n nicht prim, so ist n das Produkt von mindestens zwei (nicht notwendig verschiedenen) Primzahlen: $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, $k \geq 2$. Wegen $n \geq p_1 \cdot p_2$ können p_1 und p_2 nicht beide größer als $\sqrt{n}$ sein, in jedem Fall besitzt also n einen Primteiler $p \leq \sqrt{n}$.

Anwendung: $6! + 1 = 721$ prim? $\rightarrow$ prüfe Teilbarkeit durch Primzahlen $\leq [\sqrt{721}] = 26$.
Da $6! + 1$ durch kein $n \leq 6$ teilbar sein kann (warum?), muß man nur noch Teilbarkeit durch $7, 11, 13, 17, 19$ und 23 prüfen und findet sofort: $721 = 7 \cdot 103$.
$6! - 1 = 719$ hingegen ist tatsächlich durch keine Primzahl $\leq [\sqrt{719}] = 26$ teilbar und folglich selbst prim.
Daß schließlich $7! + 1 = 5041 = 71 \cdot 71$ zusammengesetzt ist, erkennt man bereits beim Ausrechnen der Wurzel.

Aufgabe 3

Die Anzahl der Nullen wird durch das größte k mit $10^k \mid 2004!$ bestimmt. Die Vielfachheit von $p = 5$ in $2004!$ ist

$$e_5(2004!) = \left[\frac{2004}{5}\right] + \left[\frac{2004}{25}\right] + \left[\frac{2004}{125}\right] + \left[\frac{2004}{625}\right] = 400 + 80 + 16 + 3 = 499$$

Da unter den Zahlen von 1 bis 2004 mehr gerade Zahlen als Vielfache von 5 sind, ist die Vielfachheit von $p = 2$ in $2004!$ sicher größer als die von $p = 5$. (Der genaue Wert ist $e_2(2004!) = 1997$, aber den muß man gar nicht ausrechnen.)

Das bedeutet: $10^{499} = 2^{499} \cdot 5^{499} \mid 2004!$, aber $10^{500} = 2^{500} \cdot 5^{500} \nmid 2004!$. Also endet die Dezimaldarstellung von $2004!$ mit genau 499 Nullen.

Aufgabe 4

a) „$\Leftarrow$“: $n = 2^k \Rightarrow \varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1}(2-1) = 2^{k-1} = \frac{n}{2}$

„$\Rightarrow$“: Es sei $n \in \mathbb{N}$ mit $\varphi(n) = \frac{n}{2}$. Die Formel $\varphi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$ liefert:

$$\prod_{p|n}(1 - \frac{1}{p}) = \prod_{p|n} \frac{p-1}{p} = \frac{1}{2} \quad \Rightarrow \quad \prod_{p|n} p = 2 \prod_{p|n} (p-1)$$

An der letzten Gleichung erkennt man:

- Die linke Seite ist gerade, 2 ist die einzige gerade Primzahl, also gilt $2 \mid n$.
- n besitzt keinen ungeraden Primteiler. Andernfalls wäre die rechte Seite durch 4 teilbar – die linke enthält aber nur einmal den Primfaktor 2.

Es folgt: 2 ist der einzige Primteiler von n, d. h. $n = 2^k$ für ein $k \in \mathbb{N}$.

b) Angenommen, es gibt ein $N \in \mathbb{N}$ mit $\varphi(N) = 14$. Dann muß für jede Primzahlpotenz p^k in der Primfaktorzerlegung von N gelten

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) \mid 14,$$

denn $\varphi(N)$ ist gerade das Produkt solcher $\varphi(p^k)$. Insbesondere muß $p - 1$ ein Teiler von 14 sein; dies ist nur für $p = 2$ oder $p = 3$ der Fall. Zusätzlich muß auch p^{k-1} ein Teiler von 14 sein, also bleiben nur die Möglichkeiten $p^k \in \{2, 2^2, 3\}$.

Wenn aber die PFZ von N keine anderen Primzahlpotenzen als diese enthalten kann, ist $N \leq 2^2 \cdot 3 = 12$; es folgt $\varphi(N) \leq N < 14$. Widerspruch!

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

4. November 2004

Einführung in die Zahlentheorie

Lösungshinweise zum 3. Übungsblatt

Aufgabe 1

Die Werte von f lassen sich mit der Möbius-Umkehrung berechnen, insbesondere gilt für Primzahlpotenzen p^k:

$$\begin{aligned} f(p^k) &= \sum_{d|p^k} \mu(d)\varphi(\frac{p^k}{d}) \\ &= \sum_{j=0}^{k} \mu(p^j)\varphi(p^{k-j}) && \text{(die Teiler von } p^k \text{ sind } 1, p, p^2, \ldots, p^k) \\ &= \mu(1)\varphi(p^k) + \mu(p)\varphi(p^{k-1}) && \text{(für } j > 1 \text{ ist } \mu(p^j) = 0) \\ &= \varphi(p^k) - \varphi(p^{k-1}) \end{aligned}$$

Für $k = 1$ ergibt sich

$$f(p) = \varphi(p) - \varphi(1) = p - 1 - 1 = p - 2,$$

und für $k > 1$ erhält man:

$$f(p^k) = (p^k - p^{k-1}) - (p^{k-1} - p^{k-2}) = p^{k-2}(p^2 - 2p + 1) = p^{k-2}(p-1)^2.$$

Damit berechnet man nun: $f(675) = f(3^3) \cdot f(5^2) = 3 \cdot 2^2 \cdot 1 \cdot 4^2 = 192$.

Wegen $f(2) = 0$ gilt für jedes ungerade (!) $n \in \mathbb{N}$: $f(2n) = f(2) \cdot f(n) = 0$. Beispiel: $f(2222222) = f(2 \cdot 1111111) = 0$.

Aufgabe 2

a) $\tau(119) = \tau(7) \cdot \tau(17) = 2 \cdot 2 = 4$
$\sigma(119) = \sigma(7) \cdot \sigma(17) = 8 \cdot 18 = 144 < 2 \cdot 119 \rightarrow$ defizient

$\tau(120) = \tau(2^3) \cdot \tau(3) \cdot \tau(5) = 4 \cdot 2 \cdot 2 = 16$
$\sigma(120) = \sigma(2^3) \cdot \sigma(3) \cdot \sigma(5) = 15 \cdot 4 \cdot 6 = 360 > 2 \cdot 120 \rightarrow$ abundant

$\tau(121) = \tau(11^2) = 3$
$\sigma(121) = \sigma(11^2) = 1 + 11 + 121 = 133 < 2 \cdot 121 \rightarrow$ defizient

b) $\sum_{d|n} \mu(d)\tau(\frac{n}{d}) = 1$, denn τ ist summatorische Funktion zu $f(n) \equiv 1$.

Aufgabe 3

Es sei $n \in \mathbb{N}$ mit $10 \mid n$ und $\tau(n) = 35$. Ist $p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ die Primfaktorzerlegung von n, liefert $\tau(n) = (k_1 + 1) \cdot \ldots \cdot (k_r + 1) = 35$ eine Darstellung der Zahl 35 als Produkt von Zahlen ≥ 2. Die einzigen Möglichkeiten sind $35 = 35$ und $35 = 5 \cdot 7$, n ist demnach von der Form p_1^{34} oder $p_1^4 p_2^6$. Wegen $10 \mid n$ besitzt n sicher die Primteiler 2 und 5, es bleiben also nur zwei Möglichkeiten: $n = 2^6 \cdot 5^4 = 40000$ oder $n = 2^4 \cdot 5^6 = 250000$.
(Wenn man die Aufgabe genau nimmt und negative n einbezieht, kommen natürlich noch -40000 und -250000 dazu.)

Aufgabe 4

Es sei $n \in \mathbb{N}$ die kleinste natürliche Zahl mit $\tau(n) = 100$. Ist $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ die Primfaktorzerlegung von n, so ist $\tau(n) = (k_1+1) \cdot \ldots \cdot (k_r+1)$. Die möglichen Zerlegungen von 100 in Faktoren > 1 sind:

$$100 = 50 \cdot 2 = 25 \cdot 4 = 25 \cdot 2 \cdot 2 = 20 \cdot 5 = 10 \cdot 10 = 10 \cdot 5 \cdot 2 = 5 \cdot 5 \cdot 4 = 5 \cdot 5 \cdot 2 \cdot 2$$

Eine Zerlegung in mehr als vier Faktoren ist nicht möglich, also kann n höchstens vier verschiedene Primteiler besitzen. Keiner dieser Primteiler kann größer als 7 (die vierte Primzahl) sein, denn sonst könnte man ihn in der PFZ einfach durch eine kleinere Primzahl „ersetzen“ und so ein kleineres n mit gleicher Teileranzahl erhalten (z. B. könnte man $2^9 \cdot 11^9$ zu $2^9 \cdot 3^9$ verkleinern; beide Zahlen haben 100 Teiler).
Es kommen also nur Zahlen der Form $n = 2^a 3^b 5^c 7^d$ mit $a, b, c, d \in \mathbb{N} \cup \{0\}$ in Frage. Dabei muß $a \geq b \geq c \geq d$ sein, denn sonst könnte man n bei gleicher Teilerzahl wiederum verkleinern, indem man die Exponenten vertauscht (z. B. ist $2^1 \cdot 3^4 \cdot 5^9 > 2^9 \cdot 3^4 \cdot 5^1$; beide Zahlen haben 100 Teiler).
Es bleiben nur folgende Kandidaten (vgl. die obigen Zerlegungen von 100):

$$2^{99},\ 2^{49} \cdot 3,\ 2^{24} \cdot 3^3,\ 2^{24} \cdot 3 \cdot 5,\ 2^{19} \cdot 3^4,\ 2^9 \cdot 3^9,\ 2^9 \cdot 3^4 \cdot 5,\ 2^4 \cdot 3^4 \cdot 5^3,\ 2^4 \cdot 3^4 \cdot 5 \cdot 7$$

Die meisten kann man sofort wegen der hohen Zweierpotenz als zu groß verwerfen; die kleinste dieser Zahlen ist $n = 2^4 \cdot 3^4 \cdot 5 \cdot 7 = 45360$.

Aufgabe 5

Ist N vollkommen, so ist $\sigma(N) = 2N$, und es gilt:

$$\sum_{d|N} \frac{1}{d} = \frac{1}{N} \cdot \sum_{d|N} \frac{N}{d} = \frac{1}{N} \cdot \sum_{d|N} d = \frac{1}{N} \cdot \sigma(N) = \mathbf{2}$$

(Was geschieht im zweiten Schritt? Die Summen $\sum_{d|N} \frac{N}{d}$ und $\sum_{d|N} d$ unterscheiden sich nur in der Reihenfolge der Summanden, denn mit d durchläuft auch $\frac{N}{d}$ alle Teiler von N. Man rechne das z. B. für $N = 28$ einmal konkret nach.)

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

11. November 2004

Einführung in die Zahlentheorie

Lösungshinweise zum 4. Übungsblatt

Aufgabe 1

- Wegen $29 \not\equiv 0 \bmod 73$ ist 29 sicher im Körper $\mathbb{Z}_{73}$ invertierbar. Mit Euklid findet man z. B. die Darstellung $2 \cdot 73 - 5 \cdot 29 = 1 = \mathrm{ggT}(73, 29)$, aus der folgt, daß $-5 \cdot 29 \equiv 1 \bmod 73$ ist. In $\mathbb{Z}_{73}$ gilt also $29^{-1} = -5 = \mathbf{68}$.
- $12^{16} \equiv 144^8 \equiv (-2)^8 = 4 \cdot 64 \equiv 4 \cdot (-9) = -36 \equiv 37 \bmod 73$, also $12^{16} = \mathbf{37}$ in $\mathbb{Z}_{73}$.
- $\dfrac{33^3 \cdot 44^4 + 70}{(-48) \cdot (-59)} = \ldots \textit{rechnen, reduzieren, rechnen} \ldots = \dfrac{26}{58} = \dfrac{13}{29} = 13 \cdot 68 = \mathbf{8}$ in $\mathbb{Z}_{73}$.

Aufgabe 2

(a) $(42, 49) = 7 \mid 28$, also ist die Kongruenz eindeutig mod $\frac{49}{7} = 7$ lösbar.

$$42x \equiv 28 \bmod 49 \overset{:14}{\Leftrightarrow} 3x \equiv 2 \bmod 7 \qquad \left(7 = \frac{49}{(49,14)}\right)$$
$$\overset{\cdot 5}{\Leftrightarrow} \mathbf{x \equiv 3} \bmod \mathbf{7} \qquad (5 \cdot 3 \equiv 1 \bmod 7)$$

(b) Hier kann man sofort reduzieren: $100 \equiv 1 \bmod 3$, $59 \equiv 2 \bmod 3$, also:

$$100x \equiv 59 \bmod 3 \Leftrightarrow \mathbf{x \equiv 2} \bmod \mathbf{3}$$

Fertig.

(c) Euklid liefert: $(1001, 135) = 1 = -304 \cdot 135 + 41 \cdot 1001$. Die Gleichung ist also eindeutig mod 1001 lösbar, und -304 ist invers zu 135 mod 1001. Nun formen wir um:

$$135x \equiv 833 \bmod 1001 \overset{\cdot(-304)}{\Leftrightarrow} x \equiv -253232 \bmod 1001$$

Wegen $253232 = 253 \cdot 1001 - 21 \equiv -21 \bmod 1001$ läßt sich diese Lösungsmenge noch einfacher schreiben: $\mathbf{x \equiv 21} \bmod \mathbf{1001}$.

(d) Das kann man auf die harte Tour mit Euklid rechnen, spätestens das Ergebnis sollte einen aber stutzig machen. Tatsächlich zeigt scharfes Hinsehen: $987 = 1597 - 610$, also gilt

$$987x \equiv 610 \bmod 1597 \Leftrightarrow -610x \equiv 610 \bmod 1597 \Leftrightarrow \mathbf{x \equiv -1} \bmod \mathbf{1597}.$$

(Für den letzten Schritt muß nur geprüft werden, daß 610 und 1597 teilerfremd sind. Das ist auch ohne Euklid schnell gemacht: Keiner der Primteiler 2, 5, 61 von 610 ist ein Teiler von 1597.)

Aufgabe 3

(a) $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = x^n(a_n + \frac{a_{n-1}}{x} + \cdots + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n})$

Die Summe in der Klammer konvergiert für $x \to \infty$ gegen a_n, ihr Betrag läßt sich also für genügend großes x durch eine Konstante C (z. B. $C = |a_n| + 1$) nach oben abschätzen. Es folgt $|f(x)| \leq C \cdot x^n$ für genügend große x.

(b) Es sei $\varepsilon > 0$; zu zeigen ist, daß für $n \to \infty$ der Quotient $\tau(n)/n^\varepsilon$ gegen Null geht. Nach Satz 2.15 existiert eine Konstante $C := C(\frac{\varepsilon}{2})$, so daß für alle $n \in \mathbb{N}$ $\tau(n) \leq C \cdot n^{\varepsilon/2}$ ist. Also gilt für $n \to \infty$:

$$\left|\frac{\tau(n)}{n^\varepsilon}\right| \leq \frac{C \cdot n^{\varepsilon/2}}{n^\varepsilon} = C \cdot n^{-\varepsilon/2} \to 0$$

Aufgabe 4

Es sei $n = a_0 + a_1 \cdot 10 + \cdots + a_k \cdot 10^k$. Wegen $10 \equiv -1 \bmod 11$ ist

$$n \equiv a_0 + a_1 \cdot (-1) + a_2 \cdot (-1)^2 + \cdots + a_k \cdot (-1)^k = \tilde{Q}(n) \bmod 11$$

Daraus folgt insbesondere: $11 \mid n \Leftrightarrow n \equiv 0 \bmod 11 \Leftrightarrow \tilde{Q}(n) \equiv 0 \bmod 11 \Leftrightarrow 11 \mid \tilde{Q}(n)$.

Um ein Kriterium für Teilbarkeit durch 37 zu finden, suchen wir eine Zehnerpotenz, die mod 37 einen möglichst einfachen Rest läßt. Mod 37 ist $100 \equiv -11$ und $1000 \equiv 1$. Aha! Schreiben wir also

$$n = m_0 + m_1 \cdot 1000 + m_2 \cdot 1000^2 + \cdots + m_k \cdot 1000^k$$

mit $0 \leq m_i < 1000$ für $0 \leq i \leq k$, so ist $n \equiv m_0 + m_1 + \cdots + m_k \bmod 37$. Die Zahlen m_i lassen sich einfach aus der Dezimaldarstellung von n ablesen, indem man diese bei der Einerstelle beginnend in Dreierblöcke einteilt.

Angewandt auf die 999-stellige Zahl $Z := 222\ldots2$ erhalten wir 333 solche Blöcke:

$$m_0 = m_1 = \ldots = m_{332} = 222$$

Es ist $Z \equiv 222 - 222 + 222 - \ldots + 222 = 222 \bmod 37$ (ungerade Anzahl von Summanden!), und da $222 = 6 \cdot 37$ ist, ist auch Z durch 37 teilbar. Weiterhin gilt:

- $Z \equiv Q(Z) = 999 \cdot 2 \equiv 0 \bmod 3$ bzw. $9 \quad \to Z$ ist durch 3 und 9 teilbar.
- $Z \equiv \tilde{Q}(Z) = 2 - 2 + 2 - \ldots + 2 = 2 \bmod 11 \quad \to Z$ ist nicht durch 11 teilbar.

Aufgabe 5

(a) Aus $3^2 \equiv 1 \bmod 8$ folgt für alle $n \in \mathbb{N}$: $3^{2n} = (3^2)^n \equiv 1^n = 1 \bmod 8$ sowie $3^{2n+1} = 3 \cdot 3^{2n} \equiv 3 \bmod 8$. $3^a + 3^b + 1$ muß daher kongruent mod 8 zu einer der folgenden Zahlen sein:

$$1 + 1 + 1 = 3, \quad 1 + 3 + 1 = 5, \quad 3 + 3 + 1 = 7$$

Welche Reste können Quadratzahlen mod 8 lassen? Machen wir uns möglichst wenig Arbeit: Jedes $k \in \mathbb{Z}$ ist kongruent mod 8 zu einer Zahl $+n$ oder $-n$ mit $0 \leq n \leq 4$, also ist $[k^2]_8 \in \{\, [0^2]_8, [1^2]_8, [2^2]_8, [3^2]_8, [4^2]_8 \,\} = \{\, [0]_8, [1]_8, [4]_8 \,\}$. Keine Quadratzahl kann kongruent zu 3, 5 oder 7 mod 8 sein!

(b) Daß diese Gleichung nicht erfüllbar ist, sieht man z. B. modulo 4: Für $k \in \mathbb{Z}$ ist $[k]_4 \in \{\, [0]_4, \pm[1]_4, [2]_4 \,\}$, also $[k^2]_4 \in \{\, [0^2]_4, [1^2]_4, [2^2]_4 \,\} = \{[0]_4, [1]_4\}$. Damit ist die linke Seite (beachte $4y^4 \equiv 0$) stets kongruent zu 0 oder 1 mod 4, die rechte aber zu 2 oder 3.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

18. November 2004

Einführung in die Zahlentheorie

Lösungshinweise zum 5. Übungsblatt

Aufgabe 1

(a) $$\left\{\begin{array}{rcl} 4x & \equiv & 3 \bmod 7 \\ 14x & \equiv & 8 \bmod 20 \\ 7x & \equiv & 2 \bmod 9 \end{array}\right. \iff \left\{\begin{array}{rcl} 4x & \equiv & 3 \bmod 7 \\ 7x & \equiv & 4 \bmod 10 \\ 7x & \equiv & 2 \bmod 9 \end{array}\right. \iff \left\{\begin{array}{rcl} x & \equiv & 2 \cdot 3 \equiv -1 \bmod 7 \\ x & \equiv & 3 \cdot 4 \equiv 2 \bmod 10 \\ x & \equiv & 4 \cdot 2 \equiv -1 \bmod 9 \end{array}\right.$$

Das System ist eindeutig mod $7 \cdot 10 \cdot 9 = 630$ lösbar (Chinesischer Restsatz). Spezielle Lösungen kann man sich wie im Beweis des CRS basteln, oder man geht Zeile für Zeile vor wie in Teil (b) beschrieben.

Am schnellsten führt bei diesem konkreten System allerdings inspiriertes Probieren zum Ziel: Die erste und dritte Gleichung zusammen besitzen die Lösungsmenge $x \equiv -1 \bmod 63$, also genau die Zahlen der Form $x = 63k - 1$. Und siehe da: Bereits $x = 63 - 1 = 62$ erfüllt auch die zweite Kongruenz. (So viel Glück hat man natürlich nicht immer!)

Die Lösung ist also $\mathbf{x \equiv 62} \bmod 630$.

(b) Das System ist lösbar, denn das Kriterium aus der Stundenübung ist erfüllt:

$2 \equiv 4 \bmod (6,8)$, $2 \equiv 2 \bmod (6,14)$, $2 \equiv 5 \bmod (6,9)$, $4 \equiv 2 \bmod (8,14)$, $4 \equiv 5 \bmod (8,9)$, $2 \equiv 5 \bmod (14,9)$

Die erste Gleichung liefert $x = 2 + 6r$, $r \in \mathbb{Z}$. Einsetzen in die zweite Gleichung führt auf:

$$6r \equiv 2 \bmod 8 \Leftrightarrow 3r \equiv 1 \bmod 4 \Leftrightarrow r \equiv -1 \bmod 4 \Leftrightarrow r = 4s - 1, s \in \mathbb{Z}$$

Also $x = 24s - 4$. Einsetzen in die dritte Gleichung führt auf:

$$10s \equiv 6 \bmod 14 \Leftrightarrow 5s \equiv 3 \bmod 7 \Leftrightarrow s \equiv 2 \bmod 7 \Leftrightarrow s = 7t + 2, t \in \mathbb{Z}$$

Also $x = 168t + 44$. Einsetzen in die vierte Gleichung führt auf:

$$168t \equiv -39 \bmod 9 \Leftrightarrow 6t \equiv 6 \bmod 9 \Leftrightarrow t \equiv 1 \bmod 3 \Leftrightarrow t = 3u + 1, u \in \mathbb{Z}$$

Also $x = 504u + 212$. Dies liefert die Gesamtlösung: $x \equiv \mathbf{212} \bmod 504$.

(c) Dieses System rechnet man wie in (b) geduldig durch, oder man bemerkt die spezielle Lösung $x = \mathbf{-1}$ (Tip: Nach welchem Muster sind die Zeilen gestrickt?). Sie ist eindeutig mod $[2, 3, 4, \ldots, 10] = [2, 3, 2^2, 5, 2 \cdot 3, 7, 2^3, 3^2, 2 \cdot 5] = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$.

Aufgabe 2

(a) Teilerfremd zu 33 ist jedes a, das weder durch 3 noch durch 11 teilbar ist; insgesamt sind die Ordnungen von $\varphi(33) = 20$ Zahlen zu bestimmen; jede Ordnung muß ein Teiler von 20 sein.

Die Potenzen 2^k, $k = 1, 2, 3, \ldots$ ergeben mod 33: $2, 4, 8, 16, 32, 31, 29, 25, 17, 1, \ldots$

Also ist $\mathrm{ord}_{33}(2) = 10$; die Ordnungen aller anderen Zahlen in dieser Folge errechnet man aus $\mathrm{ord}_{33}(2^k) = 10/(10, k)$, vgl. Stundenübung 4.

Die noch fehlenden Ordnungen lassen sich in analoger Weise z. B. aus den Potenzen 5^k und 7^k mod 33 bestimmen. Zusammengefaßt erhält man:

a	1	2	4	5	7	8	10	13	14	16	17	19	20	23	25	26	28	29	31	32
$\mathrm{ord}(a)$	1	10	5	10	10	10	2	10	10	5	10	10	10	2	5	10	10	10	5	2

(b) Im Falle $n = 1$ kann niemals $\mathrm{ord}_n(a) = n - 1$ gelten, denn für jedes $a \in \mathbb{Z}$ ist $\mathrm{ord}_1(a) = 1$; die Aussage ist in diesem Fall trivialerweise wahr. Es sei von nun an $n > 1$, und für $a \in \mathbb{N}$ gelte $\mathrm{ord}_n(a) = n - 1$.

Da die Ordnung von a mod n stets $\varphi(n)$ teilt und $\varphi(n) \leq n-1$ gilt, muß $\varphi(n) = n-1$ sein. Das bedeutet: Jede natürliche Zahl $< n$ ist teilerfremd zu n. Insbesondere besitzt n keine nichttrivialen Teiler, ist also prim.

Aufgabe 3

- Die zwei Lösungen von $x^2 \equiv -1$ mod 17 sind $x \equiv \pm 8! \equiv \pm\mathbf{4}$ mod 17 nach Korollar 3.10. ($4^2 = 16 \equiv -1$ kann einem natürlich auch ohne diesen Satz ins Auge fallen.)

- $30 = 2 \cdot 3 \cdot 5$. Die Faktoren 2, 3, 5 sind paarweise teilerfremd, damit gilt

$$x^2 \equiv -1 \bmod 30 \Leftrightarrow \begin{cases} x^2 \equiv -1 & \bmod 2 \\ x^2 \equiv -1 & \bmod 3 \\ x^2 \equiv -1 & \bmod 5 \end{cases}$$

nach dem CRS (bzw. Aufgabe 2 der Stundenübung). Die zweite Kongruenz des Systems ist nicht lösbar (Korollar 3.1 oder Nachrechnen: 0^2, 1^2 und 2^2 sind $\not\equiv -1$ mod 3); also besitzt auch $x^2 \equiv -1$ mod 30 keine Lösung.

- Mit $130 = 2 \cdot 5 \cdot 13$ bildet man wie oben ein äquivalentes Kongruenzsystem; diesmal läßt sich zumindest jede Zeile separat nach x auflösen (Korollar 3.1 oder Probieren, man beachte $1 \equiv -1$ mod 2):

$$x^2 \equiv -1 \bmod 130 \Leftrightarrow \begin{cases} x^2 \equiv -1 & \bmod 2 \\ x^2 \equiv -1 & \bmod 5 \\ x^2 \equiv -1 & \bmod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 & \bmod 2 \\ x \equiv \pm 2 & \bmod 5 \\ x \equiv \pm 5 & \bmod 13 \end{cases}$$

Diese vier linearen Kongruenzsysteme (eines für jede Vorzeichenkombination) löst man wie gehabt und erhält vier Lösungen mod 130: $x \equiv 47$, $x \equiv 57$, $x \equiv 73$, $x \equiv 83$.

Anmerkung: In Körpern ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Z}_p, \ldots$) und auch im Ring $\mathbb{Z}$ gilt, daß eine Gleichung n-ten Grades höchstens n Lösungen besitzt. In den Ringen $\mathbb{Z}_m$, $m \notin \mathbb{P}$, gilt dies nicht; wie wir gesehen haben, besitzt die quadratische Gleichung $x^2+1 = 0$ vier Lösungen in $\mathbb{Z}_{130}$.

Aufgabe 4

x sei wie in der Aufgabe definiert, und es sei $k \in \{1, 2, \ldots, r\}$ beliebig; wir müssen zeigen, daß $x \equiv c_k \bmod m_k$ gilt.

Für $i \neq k$ gilt $m_k \mid M_i$. Die Summe vereinfacht sich mod m_k also auf einen Summanden:

$$x = \sum_{i=1}^{r} c_i M_i^{\varphi(m_i)} \equiv c_k M_k^{\varphi(m_k)} \bmod m_k$$

m_k ist teilerfremd zu jeder der Zahlen m_i, $i \neq k$, also auch zu ihrem Produkt M_k. Mit dem kleinen Fermat folgt $M_k^{\varphi(m_k)} \equiv 1 \bmod m_k$, und übrig bleibt wie gewünscht:

$$x \equiv c_k M_k^{\varphi(m_k)} \equiv c_k \bmod m_k$$

Aufgabe 5

Wir erinnern uns ans schriftliche Dividieren. Was geschieht z. B. beim Berechnen von $1/7$?

1 geteilt durch 7 gibt 0, Rest 1. Eine 0 herunterholen, macht 10.
10 geteilt durch 7 gibt 1, Rest 3. Eine 0 herunterholen, macht 30.
30 geteilt durch 7 gibt 4, Rest 2. Eine 0 herunterholen, macht 20.
20 geteilt durch 7 gibt 2, Rest 6. Eine 0 herunterholen, macht 60. [...]

Daraus erhält man sukzessive die Dezimalentwicklung von $1/7 = 0.142\ldots$.

Für $n > 1$ kann man nach diesem Vorbild den folgenden Algorithmus formulieren.

Beginne mit $r_0 := 1$ *und definiere für* $k \in \mathbb{N}$ *„Reste“* r_k *sowie „Stellen“* c_k *rekursiv durch Division mit Rest:* $10r_{k-1} = c_k \cdot n + r_k,\ 0 \leq r_k < n$.
Dann sind alle $c_k \in \{0, 1, 2, \ldots, 9\}$, *und* $\dfrac{1}{n} = \displaystyle\sum_{k=1}^{\infty} c_k 10^{-k} =: 0.c_1c_2c_3\ldots$ *ist die Dezimalbruchentwicklung von* $1/n$.

Was hat das nun mit der Ordnung von 10 modulo n zu tun? Betrachtet man die obige Division mit Rest modulo n, sieht man, daß stets $r_k \equiv 10r_{k-1}$ gilt. Aus $r_0 = 1$ folgt so rekursiv $r_1 \equiv 10$, $r_2 \equiv 10^2$, $\ldots \Rightarrow\ r_k \equiv 10^k \bmod n$ für jedes $k \in \mathbb{N}$.

Da jeder der Reste r_k zwischen 0 und $n-1$ liegen muß, ist ihre Folge durch die Kongruenzen bereits eindeutig bestimmt. Außerdem sieht man, daß diese Folge sich spätestens im $(n-1)$-ten Schritt zu wiederholen beginnt, denn es gibt nur n verschiedene Reste, die überhaupt auftreten können. Wir können noch genauere Aussagen machen:

Ist $(10, n) = 1$, so besitzt 10 eine Ordnung L mod n. Es gilt $10^L \equiv 10^0 \bmod n$, also auch $r_L \equiv r_0 = 1 \bmod n$, wegen $0 \leq r_L < n$ also sogar $r_L = r_0 = 1$. Da die r_k rekursiv definiert sind, zieht das $r_{L+i} = r_i$ für jedes $i \in \mathbb{N}$ nach sich; die Folge $(r_k)_{k=0,1,2,\ldots}$ ist also periodisch mit der Periodenlänge L.

Nun sind wir fast fertig: Da jede Nachkommastelle c_k nur von dem Wert von r_{k-1} abhängt, ist auch die Folge $(c_k)_{k=1,2,3,\ldots}$ und damit der Dezimalbruch von $1/n$ periodisch mit der Periodenlänge L.

Gibt es eine vielleicht eine kürzere Periode als L? (Z. B. besitzt $0.\overline{313131}$ sicher eine Periode der Länge 6, die sich aber noch zur Zweierperiode $0.\overline{31}$ optimieren läßt.) Nein! Beweis: Ist $1/n = 0.\overline{c_1c_2\ldots c_r}$, so ist $(10^r - 1)/n = 10^r \cdot 1/n - 1/n$ eine ganze Zahl (nämlich?). Also gilt $n \mid (10^r - 1)$, und nach Definition der Ordnung ist $r = L$ der kleinstmögliche Exponent mit dieser Eigenschaft.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

25. November 2004

Einführung in die Zahlentheorie

Lösungshinweise zum 6. Übungsblatt

Aufgabe 1

- Da 2, 3 und 4 nicht teilerfremd zu 18 sind, ist 5 der kleinste Kandidat für eine Primitivwurzel mod 18. Tatsächlich ist $\mathrm{ord}_{18}(5) = \phi(18) = 6$, denn 5^k, $k \in \mathbb{N}$ mod 18 ergibt: $5, 7, 17, 13, 11, 1, \ldots$ Daraus erhält man nun alle weiteren Primitivwurzeln:

$$\begin{aligned} a \text{ ist PW mod } 18 &\Leftrightarrow a \equiv 5^k \bmod 18 \text{ mit } (k,6) = 1 \\ &\Leftrightarrow a \equiv \mathbf{5} \bmod 18 \text{ oder } a \equiv 5^5 \equiv \mathbf{11} \bmod 18 \end{aligned}$$

- Wegen $\phi(23) = 22$ hat jedes Element $a \in \{1, 2, \ldots, 22\}$ eine der Ordnungen $1, 2, 11$ oder 22 mod 23.

  Beim ersten Kandidaten $a = 2$ rechnet man nach: $2^{11} \equiv 1 \bmod 23$, also $\mathrm{ord}_{23}(2) = 11$ (im Kopf bestätigt man, daß 2^1 und 2^2 nicht kongruent 1 sind). Ebenso erhält man $\mathrm{ord}_{23}(3) = 11$. Die Ordnung von $4 = 2^2$ kann nicht größer sein als die von 2 (Formel aus Stundenübung 5), also kommt auch 4 nicht mehr als PW in Frage.

  Der Kandidat $a = 5$ führt dann aber zum Erfolg: mod 23 berechnet man $5^2 \equiv 2 \not\equiv 1$ und $5^{11} = 5 \cdot (5^2)^5 \equiv 5 \cdot 9 \equiv -1 \not\equiv 1$; damit muß $\mathrm{ord}_{23}(5) = 22$ sein.

  Primitivwurzeln mod 23 sind alle $a \in \mathbb{Z}$, die mod 23 kongruent zu einer der folgenden Zahlen sind: $\{5^1, 5^3, 5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, 5^{21}\}$.

  ... oder ausgerechnet: $\{5, 10, 20, 17, 11, 21, 19, 15, 7, 14\}$.

  Jedes a mit $(a, 23) = 1$ ist kongruent mod 23 zu einer der Zahlen $5^k, k \in \{1, 2, \ldots, 22\}$. (Diese Zahlen sind paarweise inkongruent mod 23.) Folglich gilt:

$$\begin{aligned} \mathrm{ord}_{23}(a) = 11 &\Leftrightarrow a \equiv 5^k \bmod 23 \text{ mit } \frac{22}{(k,22)} = 11 \\ &\Leftrightarrow a \equiv 5^k \bmod 23 \text{ mit } (k,22) = 2 \\ &\Leftrightarrow a \equiv 5^k \bmod 23 \text{ mit } k \in \{2, 4, 6, 8, \ldots, 20\} \\ &\Leftrightarrow a \equiv 5^{2k} \equiv (5^2)^k \equiv 2^k \bmod 23 \text{ mit } k \in \{1, 2, 3, \ldots, 10\} \end{aligned}$$

  Oder ausgerechnet: a hat die Ordnung 11 mod 23 genau dann, wenn a kongruent mod 23 zu einer der Zahlen $2, 4, 8, 16, 9, 18, 13, 3, 6$ oder 12 ist.

Aufgabe 2:

(a) Der Botschaft „HALLO“ entspricht die Zahlenfolge $8, 1, 12, 12, 15$. Zum Verschlüsseln müssen die 35-ten Potenzen dieser Zahlen mod 2183 berechnet werden. Wenn man keinen Computer/Taschenrechner zur Hand hat, kann man wegen $X^{35} = X^{2^5} \cdot X^2 \cdot X$

dazu die auf dem Übungsblatt bereitgestellten Quadrate mod 2183 benutzen; zum Beispiel ist $8^{32} \equiv 64^{16} \equiv 1913^8 \equiv 861^4 \equiv 1284^2 \equiv 491$. Man erhält:

$$8^{35} \equiv 347, \quad 12^{35} \equiv 1292, \quad 15^{35} \equiv 1855$$

Die verschlüsselte Folge zum Klartext „HALLO“ lautet also: $347, 1, 1292, 1292, 1855$.

(b) Es ist $\varphi(n) = 58 \cdot 36 = 2088$; zum Entschlüsseln $\tilde{X} \mapsto X \equiv \tilde{X}^t \bmod 2183$ benötigt man also ein $t \in \mathbb{N}$ mit $35 \cdot t \equiv 1 \bmod 2088$. Euklid liefert

$$(2088, 35) = 1 = 179 \cdot 35 - 3 \cdot 2088 \Rightarrow 179 \cdot 35 \equiv 1 \bmod 2088.$$

Ein Entschlüsselungsexponent ist also z. B. $t = 179$. Um 179-te Potenzen mod 2183 zu berechnen, kann man wie oben wiederholtes Quadrieren benutzen. Man erhält schließlich:

$$753^{179} \equiv 20, \quad 1347^{179} \equiv 5, \quad 520^{179} \equiv 19$$

Die Nachricht lautet: TEST TEST TEST...

Aufgabe 3

Bekannt seien die Werte n und $\varphi(n)$ sowie die Tatsache, daß $n = p \cdot q$ für gewisse Primzahlen p und q ist. Aus

$$\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1$$

folgt $p + q = n - \varphi(n) + 1$, und aus

$$(p+q)^2 - (p-q)^2 = 4pq = 4n$$

erhält man $p - q = \pm\sqrt{(p+q)^2 - 4n}$, dessen rechte Seite man nun auch ausrechnen kann, da $p + q$ bereits bekannt ist. Aus den Beziehungen $(p + q) + (p - q) = 2p$ und $(p + q) - (p - q) = 2q$ lassen sich nun p und q selbst bestimmen.

Die Zerlegung $n = p \cdot q$, die man so erhält, ist bis auf die Reihenfolge eindeutig (das sollte sie auch: PFZ!), denn unterschiedliche Vorzeichen vor der Wurzel bewirken nur einen Rollentausch zwischen p und q.
(Wir sind übrigens stillschweigend davon ausgegangen, daß $p \neq q$ ist. Andernfalls ließe sich die Zerlegung sofort durch $p = q = \sqrt{n} \in \mathbb{N}$ berechnen.)

Hintergrund dieser Aufgabe: Um den Entschlüsselungsexponenten für ein RSA-Verfahren zum Modul n zu bestimmen, muß man $\varphi(n)$ berechnen. Der direkte Weg (zähle alle zu n teilerfremden Zahlen $\leq n$) ist praktisch undurchführbar, wenn n sehr groß ist. Der bequeme Weg (Multiplikativität ausnutzen) setzt voraus, daß man über die Zerlegung $n = p \cdot q$ verfügt; auch die Faktorisierung großer Zahlen ist aber ein Problem, für das kein schneller Algorithmus bekannt ist. Nun wäre es ja trotzdem denkbar, daß sich $\varphi(n)$ noch auf eine andere Weise berechnen läßt, für die man die Zerlegung gar nicht zu kennen braucht. Doch wie wir gesehen haben, sind die Probleme „faktorisiere n“ und „berechne $\phi(n)$“ im wesentlichen äquivalent.

Aufgabe 4

Es sei $a = x^2$ mit $x \in \mathbb{N}$, und p sei eine ungerade Primzahl. Falls $p \mid a$ gilt (das kann nur für endlich viele p der Fall sein!), ist $a^{(p-1)/2} \equiv 0 \bmod p$. Gilt aber $p \nmid a$, folgt auch $p \nmid x$ (warum?) und damit $(p, x) = 1$. In diesem Fall liefert der kleine Fermat:

$$a^{\varphi(p)/2} = a^{(p-1)/2} = x^{p-1} = x^{\varphi(p)} \equiv 1 \bmod p$$

a kann also keine Primitivwurzel mod p sein.

Anmerkung: Eine 1927 von Emil Artin aufgestellte und bis heute nicht bewiesene Vermutung besagt, daß jedes $a \in \mathbb{N}$, das keine Quadratzahl ist, Primitivwurzel zu unendlich vielen Moduln $p \in \mathbb{P}$ ist. Im Falle $a = 10$ würde aus der Gültigkeit dieser Vermutung z. B. folgen, daß für unendlich viele $p \in \mathbb{P}$ der Dezimalbruch zu $1/p$ die „volle“ Periodenlänge $p - 1$ besitzt.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

2. Dezember 2004

Einführung in die Zahlentheorie

Lösungshinweise zum 7. Übungsblatt

Aufgabe 1

Es reicht, $x^2 \bmod 16$ für $0 \le x \le 15$ mit $(x, 16) = 1$ zu berechnen. (Wäre $(x, 16) \neq 1$, so auch $(x^2, 16) \neq 1$, und nach der in der Vorlesung benutzten Definition sind zur Konkurrenz „quadratischer Rest/Nichtrest“ nur zu 16 teilerfremde Zahlen zugelassen.)

Wenn man $15 \equiv -1, 13 \equiv -3$ usw. beachtet, erhält man:

$$1^2 \equiv 15^2 \equiv 1 \bmod 16, \quad 3^2 \equiv 13^2 \equiv 9 \bmod 16, \quad 5^2 \equiv 11^2 \equiv 9 \bmod 16, \quad 7^2 \equiv 9^2 \equiv 1 \bmod 16$$

Es gibt also bis auf Kongruenz genau zwei quadratische Reste mod 16, nämlich 1 und 9.

Anmerkung: Manchmal wird in der Definition von „quadratischer Rest/Nichtrest“ auf die Teilerfremdheit verzichtet. In diesem Fall würde man auch 4 und 0 als quadratische Reste bezeichnen.

—

Auch modulo 23 reicht es, ausgewählte Quadrate zu berechnen:

x	1	2	3	4	5	6	7	8	9	10	11
$x^2 \bmod 23$	1	4	9	16	2	13	3	18	12	8	6

Wegen $12 \equiv -11$ usw. muß man keine $x > 23/2$ betrachten. Quadratische Reste mod 23 sind bis auf Kongruenz genau die $(23 - 1)/2 = 11$ Zahlen in der unteren Zeile.

—

Nach den Ergänzungsgesetzen gilt:

$$\text{2 ist quad. Rest mod } p > 2 \quad \Leftrightarrow \quad \left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \bmod 8$$

$$-1 \text{ ist quad. Nichtrest mod } p > 2 \quad \Leftrightarrow \quad \left(\frac{-1}{p}\right) = -1 \Leftrightarrow p \equiv 3 \bmod 4$$

Ist $p \equiv 1 \bmod 8$, so gilt wegen $4 \mid 8$ auch $p \equiv 1 \bmod 4$; diese Zahlen genügen nicht der zweiten geforderten Kongruenz. Dagegen erfüllen alle p mit $p \equiv -1 \bmod 8$ automatisch auch $p \equiv -1 \equiv 3 \bmod 4$. Im Bereich $67 < p < 131$ findet man vier solche Primzahlen, nämlich 71, 79, 103 und 127.

Aufgabe 2

Modulo 4 gilt $p \equiv 1$ und $q \equiv 1$; mod 8 haben wir $p \equiv 1$ und $q \equiv -3$. Die Ergänzungsgesetze liefern die Werte:

$$\left(\frac{-1}{p}\right) = 1, \quad \left(\frac{-1}{q}\right) = 1, \quad \left(\frac{2}{p}\right) = 1, \quad \left(\frac{2}{q}\right) = -1$$

Das letzte Symbol müssen wir zunächst vereinfachen, zum Beispiel so:

$$\begin{aligned}
\left(\frac{q}{p}\right) = \left(\frac{613}{313}\right) &= \left(\frac{300}{313}\right) && (613 \equiv 300 \bmod 313)\\
&= \left(\frac{3}{313}\right) \cdot \left(\frac{10^2}{313}\right) && (\text{Multiplikativität})\\
&= \left(\frac{3}{313}\right) && (\text{für } p \nmid a \text{ ist stets } \left(\frac{a^2}{p}\right) = 1)\\
&= \left(\frac{313}{3}\right) && (\text{Rezi-Gesetz, beachte } 313 \not\equiv 3 \bmod 4)\\
&= \left(\frac{1}{3}\right) && (313 \equiv 1 \bmod 3)\\
&= \left(\frac{1^2}{3}\right) = \mathbf{1}
\end{aligned}$$

Die Kongruenz $x^2 \equiv -13 \equiv 300 \equiv 613 \bmod 313$ ist also lösbar; genau das besagt obiges Legendre-Symbol nach Definition.

Aufgabe 3

- Nach unserem Kriterium aus Aufgabe 3 der Stundenübung ist die quadratische Gleichung $15x^2 + 8x + 5 = 0 \bmod 13$ nicht lösbar, denn für die Diskriminante $D = 8^2 - 4 \cdot 15 \cdot 5 = -236$ dieser Gleichung gilt:

$$\left(\frac{D}{13}\right) = \left(\frac{-236}{13}\right) = \left(\frac{2}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{-1}{13}\right) = (-1) \cdot 1 = -1$$

- Hier ist $D = -399 \equiv 0 \bmod 19$; das Diskriminantenkriterium versichert uns, daß eine (doppelte) Lösung existiert. Da 19 eine Primzahl ist, gilt $x^2 \equiv 0 \bmod 19 \Leftrightarrow x \equiv 0 \bmod 19$, und wir können umformen:

$$\begin{aligned}
10x^2 + x + 10 \equiv 0 \bmod 19 &\overset{\cdot 2}{\Leftrightarrow} x^2 + 2x + 1 \equiv 0 \bmod 19\\
&\Leftrightarrow (x+1)^2 \equiv 0 \bmod 19\\
&\Leftrightarrow x \equiv -1 \bmod 19
\end{aligned}$$

  Lösungen der Kongruenz sind also alle Zahlen der Form $x = 19k - 1$, $k \in \mathbb{Z}$.

- Bevor man hier die Diskriminante berechnet, multipliziert man die Kongruenz vielleicht besser mit 5 (das ist eine Inverse von 12 mod 59), um die äquivalente, aber einfachere Gleichung $x^2 - 4x - 2 \equiv 0$ zu erhalten. Für diese Gleichung ist $D = 4^2 - 4 \cdot 1 \cdot 2 = 8$ und $\left(\frac{D}{59}\right) = \left(\frac{8}{59}\right) = \left(\frac{2}{59}\right)^3 = (-1)^3 = -1$; die Kongruenz ist also nicht lösbar.

Aufgabe 4

Da p als ungerade vorausgesetzt wurde, ist $(2, p) = 1$, und es gilt:

$$q \equiv 1 \bmod 2p \Leftrightarrow 2p \mid (q-1) \Leftrightarrow 2 \mid (q-1) \text{ und } p \mid (q-1)$$

$2 \mid (q-1)$ ist klar, weil q als Primteiler der ungeraden Zahl M_p selbst ungerade sein muß. Für die zweite Teilerbeziehung müssen wir etwas weiter ausholen:
Ist $q \neq 1$ ein Teiler von $M_p = 2^p - 1$, so ist $2^p \equiv 1 \bmod q$. Nach dem kleinen Fermat ist auch $2^{\varphi(q)} = 2^{q-1} \equiv 1 \bmod q$. Sowohl p als auch $q-1$ müssen demnach Vielfache von $\mathrm{ord}_q(2)$ sein. Wegen $p \in \mathbb{P}$ ist das aber nur möglich, wenn $p = \mathrm{ord}_q(2)$ und damit $p \mid (q-1)$ gilt.

Es bleibt noch die Kongruenz $q \equiv \pm 1 \bmod 8$ zu beweisen. Das sieht verdächtig nach einem der Ergänzungsgesetze aus. Für ungerades $q \in \mathbb{P}$ gilt nämlich:

$$q \equiv \pm 1 \bmod 8 \Leftrightarrow 2 \text{ ist quad. Rest mod } q \Leftrightarrow \exists x \in \mathbb{Z} : x^2 \equiv 2 \bmod q$$

Wie sollen wir die Lösbarkeit dieser Gleichung beweisen? Durch Hinschreiben einer Lösung! Wir wissen bereits, daß $2^p \equiv 1 \bmod q$ gilt. Daraus folgt $2 \cdot 2^p = 2^{p+1} \equiv 2 \bmod q$, und zum Glück für uns ist die linke Seite das Quadrat von $x := 2^{(p+1)/2}$ (p ist ungerade!). Fertig.

Anwendung: Bei der Suche nach Primteilern von $M_{17} = 2^{17} - 1 = 131071$ kann man sich auf Primzahlen q mit $q^2 \leq M_{17}$, $q \equiv 1 \bmod 2 \cdot 17$ und $q \equiv \pm 1 \bmod 8$ beschränken. (Für die erste Bedingung vgl. Aufgabe 2 der 2. Hausübung, die beiden anderen haben wir soeben bewiesen.)
Die Primzahlen q, die $q^2 \leq M_{17}$ und $q \equiv 1 \bmod 2 \cdot 17$ erfüllen, sind nach dem Hinweis: $103, 137, 239$ und 307. 307 ist nicht $\equiv \pm 1 \bmod 8$, die anderen Kandidaten schließt man durch Nachrechnen aus: 131071 ist durch keine dieser Zahlen teilbar.

Damit ist gezeigt, daß M_{17} eine Primzahl ist – die sechste Mersenne-Primzahl nach M_2, M_3, M_5, M_7 und M_{13}.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

9. Dezember 2004

Einführung in die Zahlentheorie

Lösungshinweise zum 8. Übungsblatt

Aufgabe 1

(a) $\left(\frac{7}{143}\right) = -\left(\frac{143}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = \mathbf{1}$

$\left(\frac{39}{35}\right) = \left(\frac{4}{35}\right) = \left(\frac{2}{35}\right)^2 = \mathbf{1}$

$\left(\frac{499}{1001}\right) = \left(\frac{1001}{499}\right) = \left(\frac{3}{499}\right) = -\left(\frac{499}{3}\right) = -\left(\frac{1}{3}\right) = \mathbf{-1}$

(b) $\mathbf{x^2 \equiv 7 \bmod 143}$ besitzt keine Lösung.

Gäbe es nämlich ein $x \in \mathbb{Z}$ mit $x^2 \equiv 7 \bmod 143$, so müste auch $x^2 \equiv 7 \bmod d$ für jeden Teiler d von $143 = 11 \cdot 13$ gelten. Nun ist aber die Kongruenz $x^2 \equiv 7 \bmod 11$ nicht lösbar, wie man z. B. an

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{2^2}{7}\right) = -1$$

sieht. (Auch mod 13 erhält man ein negatives Ergebnis.)

$\mathbf{x^2 \equiv 39 \bmod 35}$ läßt sich zu $x^2 \equiv 4 \bmod 35$ vereinfachen. Hier sieht man bereits zwei Lösungen: $x \equiv \pm 2$. Die anderen findet man durch Probieren, oder man stellt das äquivalente (Chinesischer Restsatz!) System auf:

$$x^2 \equiv 4 \bmod 35 \Leftrightarrow \begin{cases} x^2 \equiv 4 \mod 5 \\ x^2 \equiv 4 \mod 7 \end{cases} \Leftrightarrow \begin{cases} x \equiv \pm 2 \mod 5 \\ x \equiv \pm 2 \mod 7 \end{cases}$$

Das sind vier Systeme (eins für jede VZ-Kombination), die die vier Lösungen $x \equiv \pm 2$ und $x \equiv \pm 12 \bmod 35$ liefern.

$\mathbf{x^2 \equiv 499 \bmod 1001}$ ist nicht lösbar, wie uns das entsprechende Jacobi-Symbol aus Teil a) versichert.

Aufgabe 2

Alle angegebenen quadratischen Formen haben die Diskriminante $d = -59$; dies liefert uns leider noch keine Information über Äquivalenz bzw. Nichtäquivalenz[1]. Wir müssen abwarten, bis wir die reduzierten Formen bestimmt haben.

[1] Na ja, *fast* keine Information. Man könnte die Klassenzahl von -59 nachschlagen: diese beträgt 3, also sind mindestens zwei unserer quadratischen Formen äquivalent... fragt sich nur, welche.

$\mathbf{f_1(x,y) = 3x^2 + 11xy + 15y^2}$ ist nicht reduziert, denn $11 > 3$. Mit den Transformationen T_0, T_+ und T_- läßt sie sich aber in eine reduzierte Form überführen (ich gebe nur an, was mit den Koeffizienten geschieht):

$$(3, 11, 15) \overset{T_-}{\mapsto} (3, 5, 7) \overset{T_-}{\mapsto} (3, -1, 5)$$

f_1 ist also äquivalent zur reduzierten Form $\mathbf{g_1(x,y) := 3x^2 - xy + 5y^2}$.

Die zugehörige Transformationsmatrix ist $T := T_-^2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$.

Anmerkung: Zur Probe und um deutlich zu machen, daß sich hinter dieser Transformation nichts anderes als die Wahl eines geeigneten „Koordinatensystems“ verbirgt, können wir ja einmal nachrechnen, daß die Variablensubstitution $(x, y) \to (u, v)$ mit

$$\begin{pmatrix} u \\ v \end{pmatrix} := T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x - 2y \\ y \end{pmatrix}$$

tatsächlich $f_1(x, y)$ auf die soeben bestimmte reduzierte Form bringt:

$$f_1(u, v) = 3u^2 + 11uv + 15v^2 = 3(x - 2y)^2 + 11(x - 2y)y + 15y^2 = 3x^2 - xy + 5y^2 = g_1(x, y)$$

—

$\mathbf{f_2(x,y) = 35x^2 + 121xy + 105y^2}$. Wir reduzieren:

$$(35, 121, 105) \overset{T_-}{\mapsto} (35, 51, 19) \overset{T_0}{\mapsto} (19, -51, 35) \overset{T_+}{\mapsto} (19, -13, 3) \overset{T_0}{\mapsto} (3, 13, 19) \overset{T_-}{\mapsto} (3, 7, 9) \overset{T_-}{\mapsto} (3, 1, 5)$$

f_2 ist äquivalent zur reduzierten Form $\mathbf{g_2(x,y) := 3x^2 + xy + 5y^2}$.

Transformationsmatrix: $T := T_- T_0 T_+ T_0 T_-^2 = \begin{pmatrix} -2 & 5 \\ 1 & -3 \end{pmatrix}$

—

$\mathbf{f_3(x,y) = 3x^2 + 7xy + 9y^2}$. Reduzieren:

$$(3, 7, 9) \overset{T_-}{\mapsto} (3, 1, 5)$$

f_3 ist äquivalent zur reduzierten Form $\mathbf{g_3(x,y) := 3x^2 + xy + 5y^2}$.

Transformationsmatrix: $T := T_- = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

—

$\mathbf{f_4(x,y) = 3x^2 + 5xy + 7y^2}$. Reduzieren:

$$(3, 5, 7) \overset{T_-}{\mapsto} (3, -1, 5)$$

f_4 ist äquivalent zur reduzierten Form $\mathbf{g_4(x,y) := 3x^2 - xy + 5y^2}$.

Transformationsmatrix: $T := T_- = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

—

Nun können wir die Äquivalenzen klären: Ein Vergleich der reduzierten Formen ergibt $f_1 \simeq f_4$ und $f_2 \simeq f_3$, aber $f_1, f_4 \not\simeq f_2, f_3$.

Aufgabe 3:

(a) Da $b^2 - 4ac \equiv 0 \bmod 4$ (für gerades b) oder $b^2 - 4ac \equiv 1 \bmod 4$ (für ungerades b) ist, kann kein $d \in \{-1, -2, -5, -6, -9, -10, -13, -14\}$ Diskriminante einer quadratischen Form sein; für diese Zahlen ist $h(d) = 0$.

In der Vorlesung wurde die Abschätzung $\left|\frac{d}{4}\right| \leq ac \leq \left|\frac{d}{3}\right|$ für jede reduzierte quadratische Form $ax^2 + bxy + cy^2$ bewiesen; damit lassen sich zu jeder vorgebenen Diskriminante d alle möglichen reduzierten Formen f mit $d_f = d$ bestimmen. Zum Beispiel gilt für...

$\underline{d = -3}$: $\quad \frac{3}{4} \leq ac \leq 1 \Rightarrow ac = 1 \Rightarrow a = c = 1 \Rightarrow b^2 = d + 4ac = 1 \Rightarrow b = \pm 1$

Von den beiden möglichen Formen $x^2 \pm xy + y^2$ ist nur $x^2 + xy + y^2$ reduziert. Dies ist also die einzige reduzierte Form mit Diskriminante -3; alle anderen Formen mit dieser Diskriminante sind äquivalent zu $x^2 + xy + y^2$ und damit zueinander. Also

$$\begin{aligned} h(-3) &= \text{Anzahl der Äquivalenzklassen von pos. def. quad. Formen } f \text{ mit } d_f = -3 \\ &= \text{Anzahl der verschiedenen reduzierten Formen mit Diskriminante } -3 \\ &= 1 \end{aligned}$$

$\underline{d = -4}$: siehe Vorlesung, einzige reduzierte Form ist $x^2 + y^2$, also $h(-4) = 1$.

$\underline{d = -7}$: $\quad \frac{7}{4} \leq ac \leq \frac{7}{3} \Rightarrow ac = 2 \Rightarrow b^2 = 1 \Rightarrow b = \pm 1$

Bei einer reduzierten Form ist $a \leq c$ und $-a < b \leq a$, damit kommt nur $x^2 + xy + 2y^2$ in Frage, die auch wirklich reduziert ist. $\Rightarrow h(-7) = 1$

Untersucht man die restlichen Diskriminanten in derselben Weise, erhält man die Klassenzahlen und reduzierten Formen:

$h(-8) = 1 \quad (x^2 + 2y^2)$
$h(-11) = 1 \quad (x^2 + xy + 3y^2)$
$h(-12) = 2 \quad (x^2 + 3y^2 \text{ und } 2x^2 + 2xy + 2y^2)$
$h(-15) = 2 \quad (x^2 + xy + 4y^2 \text{ und } 2x^2 + xy + 2y^2)$

(b) Die reduzierten Formen zur Diskriminante -163 bestimmt man wie in Teil (a) mit der Abschätzung $163/4 \leq ac \leq 163/3$, also $41 \leq ac \leq 54$. Schreibt man $ac = 41 + k$ mit $0 \leq k \leq 13$, sieht man, daß $b^2 = -163 + 4ac = 1 + 4k$ nur für $k \in \{0, 2, 6, 12\}$ gelten kann. (Für die anderen k bekommt man keine Quadratzahl!) Die entsprechenden Werte $41, 43, 47$ und 53 für ac sind Primzahlen und lassen wegen der Forderung $a \leq c$ nur $a = 1$ zu. Da für reduzierte Formen auch $|b| \leq a$ gelten muß, folgt $b^2 = 1 + 4k \leq 1 \Rightarrow k = 1$.

Die einzige reduzierte Form mit Diskriminante $d = -163$ ist also $x^2 + xy + 41y^2$.

Anmerkung: Es wurde seit Gauß' Zeiten vermutet, daß es nur neun Diskriminanten mit der Klassenzahl 1 gibt, nämlich $-3, -4, -7, -8, -11, -19, -43, -67$ und -163. Ein Beweis, daß -163 tatsächlich das „letzte" d mit $h(d) = 1$ ist, gelang erst K. Heegner im Jahre 1952.

(c) Zu zeigen ist nur, daß für jedes solche d eine quadratische Form f mit $d_f = d$ existiert. Für $d \equiv 0 \bmod 4$ leistet $x^2 + \frac{-d}{4} y^2$ das Gewünschte, und für $d \equiv 1 \bmod 4$ kann man $x^2 + xy + \frac{-d+1}{4} y^2$ nehmen. (Diese Formen sind sogar reduziert.)

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

16. Dezember 2004

Einführung in die Zahlentheorie

Lösungshinweise zum 9. Übungsblatt

Aufgabe 1

(a) $\underline{p = 809}$: $318^2 + 1^2$ ist ein Vielfaches von p (vgl. Hinweis), genauer gilt: $\mathbf{318^2 + 1^2 = 125 \cdot 809}$.

Es sei $x = 318$, $y = 1$ und $h = 125$. Betragskleinste Reste $u \equiv x$ bzw. $v \equiv y \bmod h$ sind: $u = -57$ und $v = 1$. (Zur Erinnerung: „Betragskleinste“ bedeutet $|u|, |v| \leq h/2$. Diese Bedingung ist wichtig, sonst kann der Abstieg zu einem Aufstieg werden!)

Damit berechnet man: $(xu+yv)/h = -145$, $(xv-yu)/h = 3$. Die Methode des Abstiegs garantiert, daß die Summe der Quadrate dieser Zahlen wieder ein Vielfaches von p ist: $\mathbf{145^2 + 3^2 = 26 \cdot 809}$.

Mit den neuen Werten $x = 145$, $y = 3$, $h = 26$ beginnen wir einen weiteren Abstieg. Betragskleinste Reste mod h sind $u = -11$ bzw. $v = 3$. Damit berechnen wir: $(xu+yv)/h = -61$, $(xv-yu)/h = 18$. $\mathbf{61^2 + 18^2 = 5 \cdot 809}$, es ist also noch ein Abstieg nötig.

Mit den neuen Werten $x = 61$, $y = 18$ und $h = 5$ erhalten wir $u = 1$ sowie $v = -2$ und berechnen: $(xu + yv)/h = 5$, $(xv - yu)/h = -28$

Jetzt sind wir fertig: $\mathbf{5^2 + 28^2 = 809}$.

$\underline{p = 2053}$: Hier beginnt man mit der Darstellung (vgl. Hinweis): $\mathbf{244^2 + 1^2 = 29 \cdot 2053}$.

Ein erster Abstieg ($x = 244, y = 1, h = 29 \Rightarrow u = 12, v = 1$) führt auf $\mathbf{101^2 + 8^2 = 5 \cdot 2053}$; nochmaliger Abstieg ($x = 101, y = 8, h = 5 \Rightarrow u = 1, v = -2$) liefert $\mathbf{17^2 + 42^2 = 2053}$. Fertig!

(b) $8177 = 13 \cdot 17 \cdot 37$. Wir benutzen Identität (1) vom Stundenübungsblatt:

$$\begin{aligned} 13 \cdot 17 = \quad (2^2 + 3^2)(1^2 + 4^2) &= (2 + 12)^2 + (8 - 3)^2 = 14^2 + 5^2 \\ &= (2 - 12)^2 + (8 + 3)^2 = 10^2 + 11^2 \end{aligned}$$

Mit diesen beiden Darstellungen und Identität (1) erhält man:

$$\begin{aligned} 8177 = 13 \cdot 17 \cdot 37 = \quad (14^2 + 5^2)(1^2 + 6^2) &= (14 + 30)^2 + (84 - 5)^2 = 44^2 + 79^2 \\ &= (14 - 30)^2 + (84 + 5)^2 = 16^2 + 89^2 \\ = \quad (10^2 + 11^2)(1^2 + 6^2) &= (10 + 66)^2 + (60 - 11)^2 = 76^2 + 49^2 \\ &= (10 - 66)^2 + (60 + 11)^2 = 56^2 + 71^2 \end{aligned}$$

Bis auf Vertauschen der Summanden und Vorzeichenwechsel „unter den Quadraten“ sind dies übrigens alle Darstellungen.

(c) Wenn man das Problem nicht gleich direkt durch Probieren angehen will, kann man Identität (3) aus der Stundenübung benutzen, z. B. so:

$$\begin{aligned} 8177 &= 221 \cdot 37 \\ &= (13^2 + 6^2 + 4^2 + 0^2)(5^2 + 2^2 + 2^2 + 2^2) \\ &= (65 + 12 + 8 + 0)^2 + (26 - 30 - 8 + 0)^2 + (26 + 12 - 20 - 0)^2 + (26 - 12 + 8 - 0)^2 \\ &= 85^2 + 12^2 + 18^2 + 22^2 \end{aligned}$$

(Es gibt noch etliche andere Darstellungen.) Bei der obigen Methode muß man darauf achten, daß man nicht zu viele Nullen benutzt, denn in der Aufgabe ist nach einer Summe von vier *positiven* Quadraten gefragt. Mit $221 = 10^2+11^2+0^2+0^2$ und $37 = 6^2+1^2+0^2+0^2$ würde man beispielsweise die Darstellung $8177 = 71^2 + 56^2 + 0^2 + 0^2$ erhalten, die dieser Forderung nicht genügt.

Aufgabe 2

Wir bestimmen die zu $f(x,y) := 9x^2 + 26xy + 19y^2$ äquivalente reduzierte Form:

$$(9,26,19) \overset{T_-}{\mapsto} (9,8,2) \overset{T_0}{\mapsto} (2,-8,9) \overset{T_+}{\mapsto} (2,-4,3) \overset{T_+}{\mapsto} (2,0,1) \overset{T_0}{\mapsto} (1,0,2)$$

$f(x,y)$ ist also äquivalent zu $g(x,y) := x^2 + 2y^2$, und mit der zugehörigen Variablensubstitution

$$\begin{pmatrix} x \\ y \end{pmatrix} = T_- T_0 T_+^2 T_0 \begin{pmatrix} \bar{x} \\ \bar{y} \end{pmatrix} = \begin{pmatrix} -3\bar{x} + \bar{y} \\ 2\bar{x} - \bar{y} \end{pmatrix}$$

gilt: $f(x,y) = g(\bar{x},\bar{y})$. Wir lösen nun nicht sofort $f(x,y) = 187$, sondern die äquivalente, aber einfachere (keine gemischten Terme!) Gleichung $g(\bar{x},\bar{y}) = \bar{x}^2 + 2\bar{y}^2 = 187$.
Das geht wohl am schnellsten, indem man beachtet, daß für eine Lösung $(\bar{x},\bar{y})$ gelten muß: $2\bar{y}^2 \leq 187$, also $|\bar{y}| \leq 9$. Durchprobieren liefert nun die Darstellungen $187 = 13^2 + 2 \cdot 3^2 = 5^2 + 2 \cdot 9^2$; sämtliche ganzzahligen Lösungen von $\bar{x}^2 + 2\bar{y}^2 = 187$ sind also:

$$\begin{pmatrix} \bar{x} \\ \bar{y} \end{pmatrix} \in \left\{ \pm\begin{pmatrix} 13 \\ 3 \end{pmatrix}, \pm\begin{pmatrix} 13 \\ -3 \end{pmatrix}, \pm\begin{pmatrix} 5 \\ 9 \end{pmatrix}, \pm\begin{pmatrix} 5 \\ -9 \end{pmatrix} \right\}$$

Zum Schluß transformieren wir die Lösungen mit $x = -3\bar{x} + \bar{y}$, $y = 2\bar{x} - \bar{y}$ in unsere ursprünglichen Variablen zurück und erhalten die Lösungsmenge:

$$\begin{pmatrix} x \\ y \end{pmatrix} \in \left\{ \pm\begin{pmatrix} -36 \\ 23 \end{pmatrix}, \pm\begin{pmatrix} -42 \\ 29 \end{pmatrix}, \pm\begin{pmatrix} -6 \\ 1 \end{pmatrix}, \pm\begin{pmatrix} -24 \\ 19 \end{pmatrix} \right\}$$

Aufgabe 3

Für $x \in \mathbb{Z}$ ist x^2 kongruent modulo 8 zu 0, 1 oder 4. Jede Summe n von drei Quadraten ist also kongruent mod 8 zu einer der Zahlen 0, 1, 4, $1+1 = 2$, $1+4 = 5$, $4+4 \equiv 1$, $1+1+1 = 3$, $1+1+4 = 6$, $1+4+4 \equiv 1$ oder $4+4+4 \equiv 4$. Nur $n \equiv 7 \bmod 8$ läßt sich nicht erreichen!

Aufgabe 4

Unter welchen Umständen läßt sich eine Zahl $n \in \mathbb{N}$ *eindeutig* (bis auf Vertauschen von a und b) als Produkt $n = ab$ mit $a, b \geq 2$ darstellen? Dies ist zum einen der Fall, wenn n das Produkt zweier Primzahlen ist, zum anderen dann, wenn $n = p^3$ für ein $p \in \mathbb{P}$ ist (die einzige mögliche Faktorisierung ist in diesem Falle $n = p \cdot p^2$).
Alle anderen zusammengesetzten $n \geq 4$ lassen sich auf mindestens zwei verschiedene Weisen zerlegen; es sei $\mathcal{P}_1 := \mathbb{N}_{\geq 4} \setminus \big(\{pq \,|\, p,q \in \mathbb{P}\} \cup \{p^3 \,|\, p \in \mathbb{P}\} \big)$ die Menge dieser „mehrdeutigen“ Produkte[1]. Der Größe nach geordnet lauten die ersten Elemente dieser Menge wie folgt:

$$\mathcal{P}_1 = \{12, 16, 18, 20, 24, 28, 30, 32, 36, 40, 42, 44, 45, 48, 50, 52, 54, 56, 60, 63, 64, 66, 68, 70, 72, 76, \dots\}$$

Bezeichnen wir nun das Produkt und die Summe, die P und S mitgeteilt wurden, mit $\mathfrak{p}$ bzw. $\mathfrak{s}$ und gehen wir das Telefongespräch der Reihe nach durch.

S: Ich sehe keinen Weg, wie Sie meine Summe bestimmen können.

Mit anderen Worten: S macht P darauf aufmerksam, daß $\mathfrak{p} \in P_1$ ist. Wie kann er da so sicher sein? Wäre $\mathfrak{s}$ als Summe $\mathfrak{s} = a + b$ mit $a, b \geq 2$ und $ab \notin P_1$ darstellbar, müßte S die Möglichkeit in Betracht ziehen, daß genau dies die ursprünglichen Zahlen a und b waren, so daß P diese Zahlen leicht bestimmen kann. Ein Beispiel: Angesichts der Summe $\mathfrak{s} = 15$ könnte S nicht guten Gewissens behaupten, er sehe keinen Weg usw. , denn es könnte ja sein, daß seine Summe aus $15 = 2 + 13$ entstanden ist, und in diesem Fall hätte P das eindeutig zerlegbare Produkt $26 = 2 \cdot 13$.
Es sei nun $\mathcal{S}_1$ die Menge aller Summen, die S *garantieren*, daß P sein Produkt nicht eindeutig zerlegen kann. Dies ist genau die Menge aller Zahlen $n \geq 4$, die sich nicht als Summe $n = p + q$ oder $n = p + p^2$ mit $p, q \in \mathbb{P}$ darstellen lassen. Ihre kleinsten Elemente lauten $\mathcal{S}_1 = \{11, 17, 23, 27, 29, 35, 37, \dots\}$.

Kleine Abschweifung: Es ist kein Zufall, daß hier keine geraden Zahlen vorkommen. Die berühmte *Goldbachsche Vermutung* besagt nämlich, daß jede gerade Zahl $n \geq 4$ die Summe zweier Primzahlen ist. Diese Aussage widersetzt sich seit 250 Jahren allen Versuchen, sie zu beweisen, aber mit Hilfe von Computern wurde immerhin ihre Gültigkeit für $n \leq 4 \cdot 10^{14}$ direkt nachgeprüft. Unterstellen wir die Richtigkeit der Goldbachschen Vermutung, sehen wir, daß für $n \geq 4$ gilt: $n \notin \mathcal{S}_1 \Leftrightarrow n$ ist gerade oder $n = p + 2$ für ein $p \in \mathbb{P}$. (Oder $n = p + p^2$ für ein $p \in \mathbb{P}$, aber diese Zahlen sind stets gerade.) Daraus folgt: $n \in \mathcal{S}_1 \Leftrightarrow n$ ist ungerade und $n - 2 \notin \mathbb{P}$.

[1] Eine kürzere Beschreibung wäre $P_1 = \{n \in \mathbb{N} | \tau(n) > 4\}$.

Wir wissen bisher, daß $\mathfrak{p} \in \mathcal{P}_1$ und $\mathfrak{s} \in \mathcal{S}_1$ ist. Unseren Kenntnisstand über $\mathfrak{p}$ können wir noch aktualisieren: Zum Beispiel kann $\mathfrak{p}$ nicht 12 sein, denn die Summen $2+6$ und $3+4$, die zu den Zerlegungen $12 = 2 \cdot 6 = 3 \cdot 4$ gehören, liegen beide nicht in $\mathcal{S}_1$. Es sei $\mathcal{P}_2$ die Menge aller $n \in \mathcal{P}_1$, für die eine Zerlegung $n = ab$ mit $a, b \geq 2$ und $a + b \in \mathcal{S}_1$ existiert. Das engt den Kreis der Verdächtigen weiter ein: $\mathfrak{p} \in \mathcal{P}_2 = \{18, 24, 28, 50, 52, 54, 60, 66, 70, 72, 76 \dots\}$.

P: Danke für die Information. Ich kenne jetzt Ihre Summe.

Vor dem Anruf von S kannte P nur ihr Produkt $\mathfrak{p}$, das sich auf mehrere Weisen faktorisieren läßt. Nachdem S ihr mitgeteilt hat, sie könne seine Summe gar nicht bestimmen, weiß P, welches die richtige Zerlegung ist – wie kann das sein? Nun, mit denselben Überlegungen, die wir oben durchgeführt haben, kann P schließen, daß $\mathfrak{s} \in \mathcal{S}_1$ ist, und diese Information genügt offenbar, um alle möglichen Faktorisierungen bis auf eine auszuschließen. Wäre ihr Produkt z. B. $\mathfrak{p} = 18 = 2 \cdot 9 = 3 \cdot 6$, wüßte P in diesem Moment, daß S die Summe $2 + 9 = 11$ haben muß, denn die andere Möglichkeit $\mathfrak{s} = 3 + 6 = 9 \notin \mathcal{S}_1$ paßt nicht zur ersten Aussage von S.
Es sei $\mathcal{P}_3$ die Menge aller $n \in \mathcal{P}_2$, für die (bis auf die Reihenfolge der Faktoren) *genau* eine Zerlegung $n = ab$ mit $a, b \geq 2$ und $a + b \in \mathcal{S}_1$ existiert: $\mathfrak{p} \in \mathcal{P}_3 = \{18, 24, 28, 50, 52, 54, 76 \dots\}$

S: Jetzt kenne ich auch Ihr Produkt.

Daß $\mathfrak{p} \in \mathcal{P}_3$ gilt, weiß auch S nach Ps Antwort. Diese Information verrät ihm nun offenbar die richtige Zerlegung $s = a + b$. Es sei $\mathcal{S}_2$ die Menge aller $n \in \mathcal{S}_1$, für die (bis auf die Reihenfolge der Summanden) *genau* eine Zerlegung $n = a + b$ mit $a, b \geq 2$ und $ab \in \mathcal{P}_3$ existiert. Es muß $\mathfrak{s} \in \mathcal{S}_2$ gelten.

Damit haben wir das Gespräch vollständig ausgewertet. Unterstellen wir P und S, daß sie wissen, wovon sie reden, so kommen nur Zahlenkombinationen (a, b) in Frage, für die gilt: $a + b = \mathfrak{s} \in \mathcal{S}_2$ und $a \cdot b = \mathfrak{p} \in \mathcal{P}_3$. Beide Mengen lassen sich (notfalls mit einem Computerprogramm) im Prinzip beliebig weit auflisten. Um die Elemente von $\mathcal{S}_2$ der Reihe nach zu bestimmen, gehen wir nun die Menge $\mathcal{S}_1 \supset \mathcal{S}_2$ durch:

$11 = 2 + 9 = 3 + 8 = 4 + 7 = 5 + 6$. Von den Produkten $2 \cdot 9 = 18$, $3 \cdot 8 = 24$, $4 \cdot 7 = 28$ und $5 \cdot 6 = 30$ ist mehr als eines in $\mathcal{P}_3$, also $11 \notin \mathcal{S}_2$.

$17 = 2 + 15 = 3 + 14 = 4 + 13 = 5 + 12 = 6 + 11 = 7 + 10 = 8 + 9$. Von den zugehörigen Produkten $30, 42, 52, 60, 66, 70$ und 72 ist genau eines, nämlich 52 in $\mathcal{P}_3$. Also ist $17 \in \mathcal{S}_2$!

Damit haben wir eine passende Kombination gefunden: $a = 4$, $b = 13$, $\mathfrak{s} = 4+13 = 17$ und $\mathfrak{p} = 4 \cdot 13 = 52$. Es gibt weitere – vermutlich sogar unendlich viele – Lösungen (a, b), z. B. $(4, 61), (16, 73)$ oder $(64, 73)$. $(4, 13)$ ist jedoch (bis auf die Reihenfolge) die einzige Kombination im Bereich $a, b \leq 20$.

—

Es klingt zunächst paradox, aber wenn man die Aufgabe dahingehend umformuliert, daß P und S die Schranke $a, b \leq 20$ *mitgeteilt* wird, ist sie nicht mehr lösbar. Der Grund liegt darin, daß P und S bei dieser Variante der Geschichte nur noch Zerlegungen $\mathfrak{p} = ab$ bzw. $\mathfrak{s} = a + b$ berücksichtigen werden, für die auch $a, b \leq 20$ gilt.
Unter dieser zusätzlichen Bedingung gibt es nur noch eine Faktorisierung von $\mathfrak{p} = 52$, nämlich $4 \cdot 13$. Die Alternative $2 \cdot 26$ kann P sofort verwerfen, da der zweite Faktor zu groß ist – und schon kennt sie die richtige Zerlegung ihres Produktes! Der Anruf von S ergibt daher keinen Sinn, wenn seine Summe 17 lautet.
Nicht nur die spezielle Kombination $(4, 13)$ fällt weg, unsere Überlegungen von oben liefern, entsprechend modifiziert, tatsächlich gar keine Lösung mehr für diese Variante der Aufgabe. Erst wenn man die „öffentliche Grenze“ heraufsetzt, etwa auf $a, b \leq 100$, ist die Kombination $(4, 13)$ wieder konsistent mit dem Verlauf des Gesprächs.

—

Dieses Rätsel hat eine lange und verwickelte Geschichte. 1979 stellte Martin Gardner es unter dem Namen „The Impossible Problem“ in seiner Kolumne im *Scientific American* vor. „Impossible“, weil auf den ersten Blick zu wenig Information in der Geschichte enthalten ist, um eine eindeutige Lösung zu finden.
Allerdings hatte Gardner das Problem in der Version mit einer „öffentlichen Grenze“ (s.o.) von 100 kennengelernt und setzte diese auf 20 herunter, um es seinen Lesern einfacher zu machen. In der nächsten Ausgabe mußte er eingestehen, daß die Aufgabe dadurch wirklich *impossible* geworden war.
Dem widersprach wiederum Lee Sallows im *Mathematical Intelligencer* und bot die Lösung $(2, 6)$ für die Variante mit öffentlicher Grenze 20 an. Wie bitte? Kann S mit einer Summe von 8 ruhigen Blutes

behaupten, P habe keine Chance, seine Summe zu bestimmen? Sallows mißt der Tatsache, daß S *zuerst* anruft, große Bedeutung zu und interpretiert das Telefonat so:

S (*in Gedanken, zu sich selbst*): Meine Summe lautet 8. Wäre $8 = 3 + 5$ die richtige Zerlegung, hätte P ihr Produkt 15 sofort faktorisiert und schon lange triumphierend bei mir angerufen. Also muß $8 = 2 + 6$ oder $8 = 4 + 4$ richtig sein. In beiden Fällen hat P ein Produkt, daß sie nicht eindeutig zerlegen kann. Ich kann zwar ebensowenig ihr Produkt bestimmen wie sie meine Summe, aber wenigstens kann ich sie ein bißchen ärgern! (*greift zum Telefon, wählt Ps Nummer*) Hier ist S. Nehmen Sie's nicht persönlich... (*und so weiter)*

Hier wird in meinen Augen etwas mehr in die Aufgabe hineininterpretiert, als sie wirklich hergibt, aber immerhin führt diese Variante wieder zu einer eindeutigen Lösung.
Viele weitere Variationen des Rätsels werden in dieser umfassenden Zusammenstellung besprochen:

`http://www.mathematik.uni-bielefeld.de/~sillke/PUZZLES/logic_sum_product`

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

13. Januar 2005

Einführung in die Zahlentheorie

Lösungshinweise zum 10. Übungsblatt

Erratum: In den Lösungshinweisen zu Aufgabe 1 des 9.Übungsblattes habe ich den Fermat-Abstieg für $p = 2053$ (eine ältere Version der Aufgabe... sorry!) statt für 1553 durchgerechnet. Ich habe die korrigierten Lösungshinweise online gestellt.

Aufgabe 1

Nach dem Satz von Mertens ist $\sum_{p \le x} \frac{\log p}{p} = \log x + O(1)$ für $x \ge 2$, also gibt es eine Konstante $C > 0$, so daß für alle $x \ge 2$ gilt[1]:

$$\log x - C < \sum_{p \le x} \frac{\log p}{p} < \log x + C$$

Für $K > 1$ schätzt man nun ab:

$$\begin{aligned} \sum_{x < p \le Kx} \frac{\log p}{p} &= \sum_{p \le Kx} \frac{\log p}{p} - \sum_{p \le x} \frac{\log p}{p} \\ &> \log Kx - C - (\log x + C) \\ &= \log \frac{Kx}{x} - 2C = \log K - 2C \end{aligned}$$

Für $K \ge e^{2C}$ ist $\log K - 2C \ge 0$, und die Summe $\sum_{x < p \le Kx} \frac{\log p}{p}$ ist positiv. Daraus folgt, daß sie mindestens einen Summanden besitzt, also existiert eine Primzahl p mit $x < p \le Kx$.

Anmerkung: Man kann zeigen, daß tatsächlich zwischen x und $2x$ stets eine Primzahl liegt; dies ist das sogenannte *Postulat von Bertrand*.

Aufgabe 2

(a) Der euklidische Algorithmus mit $a = 1051$ und $b = 621$ liefert:

$$\begin{aligned} 1051 &= \mathbf{1} \cdot 621 + 430 \\ 621 &= \mathbf{1} \cdot 430 + 191 \\ 430 &= \mathbf{2} \cdot 191 + 48 \\ 191 &= \mathbf{3} \cdot 48 + 47 \\ 48 &= \mathbf{1} \cdot 47 + 1 \\ 47 &= \mathbf{47} \cdot 1 \end{aligned}$$

[1] Zur Erinnerung: Eine Funktion ist ein $O(1)$ genau dann, wenn sie beschränkt ist.

Die gesuchte Kettenbruchdarstellung ist: $1051/621 = \langle 1; 1, 2, 3, 1, 47\rangle$.

Die Näherungsbrüche p_k/q_k berechnet man daraus durch „Abschneiden“ des Kettenbruchs oder bequemer mit Hilfe der Rekursionsformeln (s. Stundenübung); sie lauten der Reihe nach:

$$\frac{1}{1}, \frac{2}{1}, \frac{5}{3}, \frac{17}{10}, \frac{22}{13}, \frac{1051}{621}$$

(b) Mit dem Taschenrechner bestimmt man den Beginn der Kettenbruchentwicklung $\alpha = \langle 1, 3, 1, 1, 1, 9, 2, \dots\rangle$ und berechnet daraus die Näherungsbrüche:

$$\frac{p_0}{q_0} = \frac{1}{1}, \frac{p_1}{q_1} = \frac{4}{3}, \frac{p_2}{q_2} = \frac{5}{4}, \frac{p_3}{q_3} = \frac{9}{7}, \frac{p_4}{q_4} = \frac{14}{11}, \frac{p_5}{q_5} = \frac{135}{106}, \frac{p_6}{q_6} = \frac{284}{223}, \dots$$

$p_4/q_4 = 14/11$ ist die beste Approximation $\alpha \approx p/q$ mit $q < q_5 = 106$, also erst recht die beste mit $q < 100$.

Der erste Näherungsbruch mit einem Fehler $< 5 \cdot 10^{-5}$ ist $\frac{p_5}{q_5}$; hier schätzt man ab:

$$|\alpha - \frac{p_5}{q_5}| \le \frac{1}{q_5 q_6} = \frac{1}{23638} < 5 \cdot 10^{-5}$$

(c) Im folgenden sei $\alpha > 0$ vorausgesetzt (sonst wird die Aufgabe kniffliger, als ich beabsichtigt hatte).

$1 + \alpha = 1 + a_0 + \dfrac{1}{a_1 + \frac{1}{a_2 + \dots}} = \langle a_0 + 1; a_1, a_2, \dots\rangle$

$\{\alpha\} = \alpha - [\alpha] = \alpha - a_0 = \langle 0; a_1, a_2, \dots\rangle$

Falls $a_0 \neq 0$, ist $\dfrac{1}{\alpha} = \dfrac{1}{a_0 + \frac{1}{a_1 + \dots}} = \langle 0; a_0, a_1, \dots\rangle$

Falls $a_0 = 0$, ist $\dfrac{1}{\alpha} = \dfrac{1}{0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}} = a_1 + \dfrac{1}{a_2 + \dots} = \langle a_1; a_2, \dots\rangle$

Aufgabe 3

(a) Die Folge der Näherungsbrüche für π ist

$$\frac{3}{1}, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \frac{103993}{33102}, \dots$$

Daran liest man ab: $\pi \approx \frac{22}{7}$ ist die beste rationale Näherung mit einem Nenner < 106 (also erst recht die beste mit einem Nenner < 10), und $\pi \approx \frac{355}{113}$ ist die beste Näherung mit einem Nenner < 33102 (also erst recht die beste mit einem Nenner < 10000). Diese Näherungen waren chinesischen Mathematikern bereits 500 n. Chr. bekannt.

Anmerkung: Der Näherungsbruch $\frac{p_3}{q_3} = \frac{355}{113}$ ist besonders „effizient“ in dem Sinne, daß ein kleinerer Fehler erst mit einem wesentlich größeren Nenner (dem Nenner 33102 des nächsten Näherungsbruchs) erreicht werden kann.
Da $q_{k+1} = a_{k+1} \cdot q_k + q_{k-1} > a_{k+1} \cdot q_k$ ist, erhält man effiziente Näherungen, indem man die Kettenbruchentwicklung direkt vor einem möglichst großen Teilnenner a_{k+1} abschneidet (so wie hier vor $a_4 = 292$.)

(b) Aus $\alpha = \langle\, 0; 4, 7, 1, 3, 6, \ldots \,\rangle$ berechnet man die ersten sechs Näherungsbrüche

$$\frac{0}{1}, \frac{1}{4}, \frac{7}{29}, \frac{8}{33}, \frac{31}{128}, \frac{194}{801}$$

Der Nenner des nächsten Näherungsbruchs ist mindestens $1 \cdot 801 + 128$, also in jedem Fall größer als 1000. Folglich ist $\alpha \approx \frac{194}{801}$ die beste Näherung mit einem Nenner < 1000.

Anmerkung: Die bekannte „Schaltjahrregel“ des Gregorianischen Kalenders erhält man, indem man die Näherung $\frac{194}{801}$ zu $\frac{194}{800} = \frac{97}{400} = \frac{1}{4} - \frac{3}{400}$ verschlechtert. Um die Diskrepanz des astronomischen Jahres zu 365 Tagen annähernd aufzufangen, muß alle vier Jahre ein zusätzlicher Tag eingeschoben werden; von diesen Schalttagen müssen aber in 400 Jahren drei Stück ausfallen. Deshalb sind die Jahre N mit $N \equiv 0 \bmod 100$ keine Schaltjahre, es sei denn $N \equiv 0 \bmod 400$.

(c) Mein Taschenrechner liefert hier mit dem Algorithmus aus Stundenübung 3:

$$\pi^4 = \langle 97; 2, 2, 3, 1, 16606, \ldots \rangle$$

Nach dem falschen Teilnenner 16606 hat es keinen Sinn, noch weiterzurechnen, denn wenn die Rundungsfehler bereits so groß sind, daß sie den ganzzahligen Anteil von ϑ_k derart verfälschen, kann man den gebrochenen Teil $\{\vartheta_k\}$, den man für die nächsten Schritte braucht, ebensogut auswürfeln.

Daß die Berechnung hier bereits so früh scheitert, liegt an dem großen Teilnenner $[\vartheta_5] = 16539$, für den man $\vartheta_5 = \frac{1}{\{\vartheta_4\}} = \frac{1}{0.0000827\ldots}$ berechnen muß. Die Aufgabe, $f(x) := 1/x$ für kleine $|x|$ numerisch zu bestimmen, ist aber sehr empfindlich gegenüber Rundungsfehlern, denn für $x \to 0$ geht $|f'(x)|$ gegen ∞.

Anmerkung: Bei dieser Aufgabe kann man auch einiges über das Innenleben seines Taschenrechners erfahren, darum hier noch etwas zum Nachdenken: Wenn ich π^4 nicht mit der x^y-Taste, sondern durch zweimaliges Anwenden der „Quadrat“-Taste berechne, bekomme ich als fünften Teilnenner den immer noch falschen, aber wesentlich besseren Wert 16540. Was geht hier vor?

(d) Mit dem „wahren“ Kettenbruch aus der Aufgabe berehnet man die Näherungsbrüche

$$\frac{97}{1}, \frac{195}{2}, \frac{487}{5}, \frac{1656}{17}, \frac{2143}{22}, \frac{35444733}{363875}, \ldots$$

Die Näherung $\pi^4 \approx 2143/22$ ist die beste mit einem Nenner $q < 363875$. Ihr Fehler beträgt höchstens $|\pi^4 - 2143/22| \le 1/(22 \cdot 363875) \approx 1.25 \cdot 10^{-7}$.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT HANNOVER

Prof. Dr. Sander
Dr. Viergutz
Marco Schwiering

20. Januar 2005

Einführung in die Zahlentheorie

Lösungshinweise zum 11. Übungsblatt

Aufgabe 1

(a) Mit einer exakten Rechnung wie in Aufgabe 1 der Stundenübung oder (im Falle von $\sqrt{5}$) mit der dort bewiesenen Formel für $\sqrt{a^2+1}$ erhält man die Kettenbrüche $\sqrt{3} = \langle 1; \overline{1,2} \rangle$ und $\sqrt{5} = \langle 2; \overline{4} \rangle$.

Für $\sqrt{a^2+2a}$ schätzt man zunächst ab:

$$a^2 < a^2 + 2a < a^2 + 2a + 1 = (a+1)^2 \;\Rightarrow\; a < \sqrt{a^2+2a} < a+1$$

Nun führt man den Algorithmus zur Kettenbruchentwicklung durch:

$$\begin{aligned}
\vartheta_0 &:= \sqrt{a^2+2a} && \Rightarrow \quad a_0 = [\vartheta_0] = a \\
\vartheta_1 &= \frac{1}{\sqrt{a^2+2a}-a} = \frac{\sqrt{a^2+2a}+a}{2a} = 1 + \frac{\sqrt{a^2+2a}-a}{2a} && \Rightarrow \quad a_1 = [\vartheta_1] = 1 \\
\vartheta_2 &= \frac{2a}{\sqrt{a^2+2a}-a} = \frac{2a(\sqrt{a^2+2a}+a)}{2a} = \sqrt{a^2+2a}+a && \Rightarrow \quad a_2 = [\vartheta_2] = 2a \\
\vartheta_3 &= \frac{1}{\sqrt{a^2+2a}-a} = \vartheta_1 && \Rightarrow \quad \text{ab hier periodisch!}
\end{aligned}$$

Also ist $\sqrt{a^2+2a} = \langle a; \overline{1, 2a} \rangle$.

(b) $\dfrac{11-\sqrt{14}}{4} = \langle 1; 1, 4, \overline{2, 1, 1, 5} \rangle$

(c) Aus $\langle 2; 2, 2, 2, \dots \rangle = 2 + \dfrac{1}{\langle 2; 2, 2, \dots \rangle}$ folgt, daß $\alpha = \langle \overline{2} \rangle$ die Gleichung $\alpha = 2 + \frac{1}{\alpha}$ erfüllt; hieraus gewinnt man die quadratische Gleichung $\alpha^2 - 2\alpha - 1 = 0$ und den Wert $\alpha = 1 + \sqrt{2}$.

Um $\alpha = \langle 1; 2, \overline{1, 2, 1} \rangle$ zu bestimmen, berechnet man zunächst $\beta = \langle \overline{1, 2, 1} \rangle$ anhand der Gleichung

$$\beta = 1 + \frac{1}{2 + \frac{1}{1+\frac{1}{\beta}}} \;\Leftrightarrow\; \beta^2 - \frac{2}{3}\beta - 1 = 0 \overset{\beta>0}{\Leftrightarrow} \beta = \frac{1+\sqrt{10}}{3}$$

und daraus

$$\alpha = 1 + \frac{1}{2+\frac{1}{\beta}} = \frac{3\beta+1}{2\beta+1} = \frac{10-\sqrt{10}}{5}$$

Aus $10 - 5\alpha = \sqrt{10}$ gewinnt man durch Quadrieren und Vereinfachen z. B.:

$$f(\alpha) := 5\alpha^2 - 20\alpha + 18 = 0$$

Aufgabe 2

Wegen $\left|\alpha - \frac{98}{67}\right| < \frac{1}{2 \cdot 67^2}$ ist $\frac{98}{67} = \langle 1; 2, 6, 5\rangle = \langle 1; 2, 6, 4, 1\rangle$ Näherungsbruch von α. Die Kettenbruchdarstellung von α beginnt also mit $\langle 1; 2, 6, 5, \dots\rangle$ (dann ist $98/67 = p_3/q_3 \geq \alpha$) oder mit $\langle 1; 2, 6, 4, 1, \dots\rangle$ (dann ist $98/67 = p_4/q_4 \leq \alpha$).

Aufgabe 3

(a) Die ersten 16 Fibonacci-Zahlen lauten:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987$$

(b) $1/1 = \langle 1\rangle$, $2/1 = \langle 2\rangle$, $3/2 = \langle 1; 2\rangle$, $5/3 = \langle 1; 1, 2\rangle$, $8/5 = \langle 1; 1, 1, 2\rangle$ $\rightarrow$ Vermutung:

$$\begin{aligned} F_{n+1}/F_n &= \langle \underbrace{1\,; \dots, 1}_{n-2}, 2\rangle \quad \text{(normierte Darstellung)} \\ \text{oder äquivalent:}\quad F_{n+1}/F_n &= \langle \underbrace{1\,; \dots, 1, 1, 1}_{n}\rangle \end{aligned}$$

für $n \geq 2$ (die zweite Kettenbruchdarstellung deckt auch noch den Fall $n = 1$ ab).

Diese Vermutung läßt sich beweisen, indem man die Rekursionsformel für die F_n benutzt, z. B. lautet der euklidische Algorithmus für F_{n+1} und F_n:

$$\begin{aligned} F_{n+1} &= \mathbf{1} \cdot F_n + F_{n-1} \\ F_n &= \mathbf{1} \cdot F_{n-1} + F_{n-2} \\ &\dots \\ F_4 = 3 &= \mathbf{1} \cdot 2 + 1 \\ F_3 = 2 &= \mathbf{2} \cdot 1 \end{aligned}$$

In jeder Zeile steht wirklich eine Division mit Rest (zur Erinnerung: der Rest muß kleiner als der Divisor sein!), denn für $n \geq 2$ ist $F_n = F_{n-1} + F_{n-2} \geq F_{n-1} + 1 > F_{n-1}$.

(c) Aus Teil (b) folgt, daß F_{n+1}/F_n der n-te Näherungsbruch von $\langle 1; 1, 1, 1, \dots\rangle$ ist. Die Folge dieser Brüche konvergiert gegen $\langle 1; 1, 1, 1, \dots\rangle$, und das ist bekanntlich (Stundenübung!) der goldene Schnitt.