Universität Bonn
Mathematisches Institut
Dr. Michael Welter

Übungen zum
Vorkurs Mathematik für Studienanfänger
2007

Einige Zeichen und Konventionen:
$\mathbb{N} := \{1, 2, 3, 4, \ldots\}$ – Die Menge der natürlichen Zahlen
$\mathbb{N}_0 := \mathbb{N} \cup \{0\}\{0, 1, 2, 3, 4, \ldots\}$
$\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, 3, 4, \ldots\}$ – Die Menge der ganzen Zahlen
$\mathbb{Q}$ – Die Menge der rationalen Zahlen
$\mathbb{R}$ – Die Menge der reellen Zahlen
$\mathbb{P} := \{2, 3, 5, 7, 11, \ldots\}$ – Die Menge der Primzahlen
$\sum$ – Summenzeichen, also z.B. $\sum_{i=0}^{n} x_i = x_0 + x_1 + \ldots + x_n$
$\prod$ – Produktzeichen, also z.B. $\prod_{i=0}^{n} x_i = x_0 \cdot x_1 \cdot \ldots \cdot x_n$
Ein leeres Produkt ist gleich 1, eine leere Summe 0.

***

Die Übungen finden in 8 verschiedenen Gruppen jeweils in der Zeit von 14 – 16 Uhr bzw. 15 – 17 Uhr statt.

Die Orte der Übungsgruppen sind:
Kleiner Hörssal, Zeichensaal (15–17): Wegelerstr. 10
Seminarräume A und B (14–16): Beringstr. 4
Seminarraum C (14–16): Beringstr. 1
Seminarräume D, E und F (14–16): Meckenheimer Allee 160, Zugang nur über Beringstr. 1

Tragen Sie sich bitte in die Listen im Glasgang ein!!!

Die Übungszettel gibt es unter http://www.math.uni-bonn.de/people/welter/lehre.html

Am Freitag, den 21.09., gibt es anstelle der Vorlesung eine **Studienberatung** und Informationen zum Thema **Auslandsstudium**.

Die folgenden Aufgaben sind für **Dienstag, den 11.09.,** vorzubereiten:

Aufgabe 1: Es seien A und B Aussagen. Wir definieren neue Aussagen $A \wedge B, A \vee B, \neg A$: Die Aussage $A \wedge B$ ist genau dann wahr, wenn die beiden Aussagen A und B wahr sind, die Aussage $A \vee B$ ist genau dann wahr, wenn mindestens eine der beiden Aussagen A und B wahr ist und die Aussage $\neg A$ ist genau dann wahr, wenn A falsch ist. Fertigen Sie Wahrheitstafeln für die Aussagen

(i) $A \wedge B, A \vee B$ und $\neg A$,

(ii) $(\neg B) \Rightarrow (\neg A)$,

(iii) $\neg((\neg B) \wedge A)$

an.

Aufgabe 2: Beweisen Sie mittels vollständiger Induktion:

(i) Für $n \geq 1$ gilt

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}.$$

(ii) Für $n \geq 3$ gilt

$$\sum_{k=1}^{n-1} \frac{2^{k+1}}{k} < \frac{2^{n+2}}{n}.$$

Aufgabe 3: Beweisen Sie mittels vollständiger Induktion, dass für alle $n \in \mathbb{N}$ und alle $q \in \mathbb{R}, q \neq 1$, gilt

$$\sum_{k=0}^{n-1} q^k = \frac{q^n - 1}{q - 1}.$$

Folgern Sie hieraus für $a, b \in \mathbb{R}$

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

Was ergibt sich für $n = 2$?

Die folgenden Aufgaben sind für **Mittwoch, den 12.09.,** vorzubereiten:

Aufgabe 4: (Binomialkoeffizienten)
Die Fakultät $n!$ ist für $n \in \mathbb{N}_0$ rekursiv definiert durch $0! := 1$ und $n! := n \cdot (n-1)!$. Weiter definieren wir für $m \in \mathbb{N}_0$ und $k \in \{0, 1, 2, \ldots, m\}$ den Binomialkoeffizienten $\binom{m}{k}$ (lies: m über k) durch

$$\binom{m}{k} := \frac{m!}{(m-k)!k!}.$$

Zeigen Sie die folgenden Aussagen

(i) $\binom{m}{k} = \binom{m}{m-k}$.

(ii) $\binom{m+1}{k+1} = \binom{m}{k+1} + \binom{m}{k}$.

(iii) $\binom{m}{k} \in \mathbb{N}$.

Aufgabe 5: Es sei $n \in \mathbb{N}$. Zeigen Sie:

(i) Für $a, b \in \mathbb{R}$ gilt:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Diese Aussage bezeichnet man als den binomischen Lehrsatz.

(ii) Für $k \in \{0, \ldots, n\}$ gilt $\binom{n}{k} \leq 2^n$.

Aufgabe 6:

(i) Zeigen Sie, dass sich jede ungerade Zahl $n \geq 3$ als Differenz von zwei aufeinanderfolgenden Quadratzahlen darstellen läßt.

(ii) Bestimmen Sie alle Darstellungen der Zahlen 15, 19, 27 als Differenz von zwei (nicht notwendigerweise aufeinanderfolgenden) Quadratzahlen.
Bemerkung: Geben Sie ein Argument an, warum Sie wirklich alle Darstellungen gefunden haben.

(iii) Zeigen Sie, dass eine ungerade Zahl $n \geq 3$ genau dann Primzahl ist, wenn sie nur eine Darstellung als Differenz von zwei Quadratzahlen besitzt.

Die folgenden Aufgaben sind für **Donnerstag, den 13.09.,** vorzubereiten:

Aufgabe 7:

(i) Es seien $n, m \in \mathbb{Z}$ und $d := \mathrm{ggT}(n, m)$. Zeigen Sie: $\mathrm{ggT}\left(\frac{n}{d}, \frac{m}{d}\right) = 1$, d.h. $\frac{n}{d}$ und $\frac{m}{d}$ sind teilerfremd.

(ii) Bestimmen Sie ein Tupel (x, y) ganzer Zahlen, so dass

$$4641x + 6615y = 105.$$

Aufgabe 8: (Die Fibonacci–Zahlen)
Die Folge $(f_n)_{n\in\mathbb{N}_0}$ der sog. *Fibonacci–Zahlen* ist rekursiv definiert durch die Vorschrift $f_0 := 0, f_1 := 1$ und $f_n := f_{n-1} + f_{n-2}$ für $n \geq 2$. Weiter seien $a := \frac{1}{2}(1 + \sqrt{5})$ und $b := \frac{1}{2}(1 - \sqrt{5})$, so dass a und b offensichtlich die Lösungen der quadratischen Gleichung $x^2 - x - 1 = 0$ sind. Die Folge $(g_n)_{n\in\mathbb{N}_0}$ sei definiert durch

$$g_n := \frac{1}{\sqrt{5}}(a^n - b^n),$$

wobei $x^0 := 1$ für jede reelle Zahl $x \neq 0$ ist.

(i) Berechnen Sie $f_0, f_1, f_2, \ldots, f_{10}$.

(ii) Berechnen Sie $g_0, g_1, g_2, \ldots, g_{10}$.

(iii) Zeigen Sie, dass $g_n = g_{n-1} + g_{n-2}$ für $n \geq 2$ gilt. Folgt hieraus $f_n = g_n$ für alle $n \in \mathbb{N}$?

Aufgabe 9: Es bezeichne $\tau(n)$ die Anzahl der positiven Teiler der natürlichen Zahl n und $\nu_p(n)$ die Vielfachheit von p in n, also den Exponenten der Primzahl p in der Primfaktorzerlegung von n.

(i) Zeigen Sie: $\tau(n) = \prod_{p\in\mathbb{P}} (\nu_p(n) + 1)$.

(ii) Bestimmen Sie alle Vielfachen von 12 mit genau zwei Primteilern und genau 14 Teilern.

(iii) Bestimmen Sie alle Vielfachen von 30 mit genau 30 Teilern.

Die folgenden Aufgaben sind für **Freitag, den 14.09.,** vorzubereiten:

Aufgabe 10:

(i) Es seien $m_1, \ldots, m_k \in \mathbb{Z}$ paarweise teilerfremd, $m := m_1 \cdot \ldots \cdot m_k$ und $a, b \in \mathbb{Z}$. Zeigen Sie:

$$a \equiv b \pmod{m_\ell} \text{ für } \ell = 1, \ldots, k \iff a \equiv b \pmod{m}$$

(ii) Falls für $a_i, b_i \in \mathbb{Z}$ die Kongruenzen

$$a_i \equiv b_i \pmod{m} \text{ für } i = 1, \ldots, n$$

gültig sind, so gilt auch

$$\begin{aligned} \sum_{i=1}^{n} a_i &\equiv \sum_{i=1}^{n} b_i \pmod{m} \\ \prod_{i=1}^{n} a_i &\equiv \prod_{i=1}^{n} b_i \pmod{m}. \end{aligned}$$

Aufgabe 11: (Teilbarkeitskriterien)
Es sei $a = \sum_{k=0}^{n} a_k \cdot 10^k$ die Dezimalentwicklung der Zahl $a \in \mathbb{N}$ und $s := \sum_{k=0}^{n} a_k$ ihre Quersumme. Zeigen Sie mit der vorhergehenden Aufgabe:

$$\begin{aligned} 3|a &\Leftrightarrow 3|s \\ 9|a &\Leftrightarrow 9|s. \end{aligned}$$

Gibt es eine ähnliche Regel für die Division durch 11?

Aufgabe 12: (Der kleine Satz von Fermat)

(i) Zeigen Sie, dass für alle $a, b \in \mathbb{Z}$ und Primzahlen p

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

gilt. Was gilt also (induktiv) für $(a_1 + a_2 + \ldots + a_n)^p$?
Tipp: Man überlege sich, dass $\binom{p}{k} \equiv 0 \pmod{p}$ für $1 \leq k \leq p-1$ und wende den Binomischen Lehrsatz an.

(ii) Folgern Sie hieraus: Für alle $a \in \mathbb{Z}$ gilt $a^p \equiv a \pmod{p}$.

Hinweis: Man betrachte zunächst den Fall $a \geq 0$ und führe dann den Fall $a < 0$ auf diesen zurück. Dabei unterscheide man die Fälle $p = 2$ und p ungerade.

Die folgenden Aufgaben sind für **Montag, den 17.09.,** vorzubereiten:

Aufgabe 13:

(i) Zeigen Sie, dass $M_k := 2^k - 1$ höchstens dann eine Primzahl ist, wenn k eine Primzahl ist.

(ii) Es seien nun p und q Primzahlen. Zeigen Sie: Ist p ein Primteiler von M_q, so gilt $p \equiv 1 \mod q$.

(iii) Der kleinste mögliche Primteiler von M_{251} ist also 503. Zeigen Sie, dass 503 tatsächlich ein Teiler von M_{251} ist.

Bemerkung: Primzahlen der Form $M_p = 2^p - 1$ nennt man Mersenne-Primzahlen. Die größte bekannte Mersenne-Primzahl (und die größte bekannte Primzahl überhaupt) ist $M_{32582657}$ (Quelle: http://www.mersenne.org).

Aufgabe 14: (Goldbachs Beweis des Satzes von Euklid)
Für $n \in \mathbb{N}_0$ sei $F_n := 2^{2^n} + 1$ die sogenannte n–te Fermat-Zahl.

(i) Zeigen Sie, dass $F_n - 2 = \prod_{i=0}^{n-1} F_i$ für alle $n \in \mathbb{N}$ gilt.

(ii) Folgern Sie hieraus, dass für je zwei $i, j \in \mathbb{N}$ mit $i \neq j$ die Zahlen F_i und F_j teilerfremd sind, dass also $\mathrm{ggT}(F_i, F_j) = 1$ ist.

(iii) Folgern Sie hieraus, dass es unendlich viele Primzahlen gibt.

Bemerkung: Es ist per definitionem $a^{b^c} = a^{(b^c)}$.

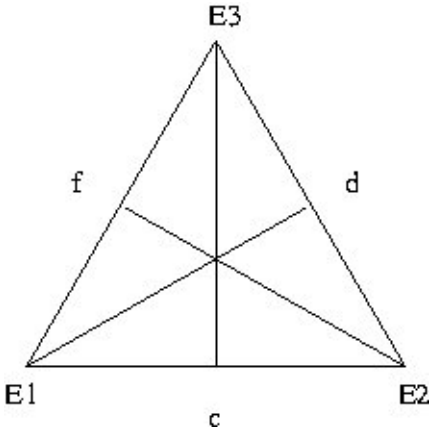
Aufgabe 15: (Aus einem chinesischen Rechenbuch)
Eine Bande von 17 Räubern stahl einen Sack mit Goldstücken. Als sie ihre Beute in gleiche Teile teilen wollten, blieben 3 Goldstücke übrig. Beim Streit darüber, wer ein Goldstück mehr erhalten sollte, wurde ein Räuber erschlagen. Jetzt blieben bei der Verteilung 10 Goldstücke übrig. Erneut kam es zum Streit, und wieder verlor ein Räuber sein Leben. Jetzt liess sich endlich die Beute gleichmäßig verteilen. Wie viele Goldstücke waren mindestens im Sack?

Die folgenden Aufgaben sind für **Dienstag, den 18.09.,** vorzubereiten:

Aufgabe 16: Prüfen Sie auf Assoziativität und Kommutativität:

$$\begin{aligned}
(\mathbb{Q}, \diamond) \qquad & \text{mit } x \diamond y := \frac{x+y}{2} \\
(\mathbb{Z}, -) \qquad & \\
(\mathbb{N}, \star) \qquad & \text{mit } x \star y := x^y \\
(\mathbb{N}, \triangle) \qquad & \text{mit } x \triangle y := x \\
(\{-1, 0, 1\}, \heartsuit) \qquad & \text{mit } x \heartsuit y := x \cdot y^3 \quad \text{(Verknüpfungstafel)}
\end{aligned}$$

Aufgabe 17:



Wir betrachten die Deckbewegungen des gleichseitigen Dreiecks $E_1E_2E_3$:

D_{120}	Drehung um 120 Grad (entgegen dem Uhrzeigersinn)
D_{240}	Drehung um 240 Grad
D_0	Drehung um 0 Grad
W_c, W_d, W_f	Wendungen um die entsprechende Achse

Stellen Sie eine Verknüpfungstafel für $(\{D_0, D_{120}, D_{240}, W_c, W_d, W_f\}, \star)$ auf, wobei $\star$ die Hintereinanderausführung der Deckbewegungen sei. Suchen Sie in der Tafel neutrale und inverse Elemente. Untersuchen Sie die Verknüpfung auf Kommutativität.

Aufgabe 18: Es seien $a, b, c, d \in \mathbb{R}$. Ein Schema

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

bezeichnet man als (zweireihige) Matrix (reeller Zahlen). Die Menge aller zweireihigen Matrizen reeller Zahlen bezeichnen wir mit $M_2(\mathbb{R})$. Die Determinante dieser Matrix ist gegeben durch

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

Für zwei Matrizen

$$M_1 := \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \text{ und } M_2 := \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

sei das Produkt der Matrizenmultiplikation definiert durch

$$M_1 \cdot M_2 := \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}.$$

Zeigen Sie:

(i) $(M_2(\mathbb{R}), \cdot)$ ist assoziativ, aber nicht kommutativ. Es existiert ein neutrales Element, aber nicht jedes Element besitzt ein Inverses.

(ii) Für $M_1, M_2 \in M_2(\mathbb{R})$ gilt $\det(M_1 \cdot M_2) = \det M_1 \cdot \det M_2$.

Die folgenden Aufgaben sind für **Mittwoch, den 19.09.,** vorzubereiten:

Aufgabe 19: Es bezeichne $M_2(\mathbb{Z})$ die Menge aller zweireihigen Matrizen ganzer Zahlen (d.h. $a, b, c, d \in \mathbb{Z}$) und Γ sei die Menge aller $A \in M_2(\mathbb{Z})$ mit $\det A = 1$. Zeigen Sie, dass $(\Gamma, \cdot)$ eine unendliche, nicht abelsche Gruppe ist.

Aufgabe 20: In dieser Aufgabe darf ohne Beweis benutzt werden, dass $\sqrt{2}$ irrational ist. Wir betrachten die folgende Teilmenge der rellen Zahlen $\mathbb{R}$:

$$K := \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}.$$

Zeigen Sie, dass $(K, +)$ und $(K \setminus \{0\}, \cdot)$ abelsche Gruppen sind, wobei $+$ und $\cdot$ die übliche Addition bzw. Multiplikation auf den rellen Zahlen bedeutet.
Bemerkung: Wo wird die Irrationalität von $\sqrt{2}$ benutzt?
Wir wissen, dass $\mathbb{Q}$ und $\mathbb{R}$ Körper sind. Diese Aufgabe zeigt also, dass es auch noch Körper "dazwischen" gibt, denn $\mathbb{Q} \subset K \subset \mathbb{R}$.

Aufgabe 21: (Noch einmal Fibonacci–Zahlen)
Es bezeichne f_n die $n-$te Fibonacci–Zahl (vgl. Aufgabe 8).

(i) Zeigen Sie, dass für alle $n \in \mathbb{N}_0$ gilt:

$$\begin{pmatrix} f_{n+2} & f_{n+1} \\ f_{n+1} & f_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+1}$$

(ii) Für alle $m, n \in \mathbb{N}$ gilt $f_{m+n} = f_{m-1} f_n + f_m f_{n+1}$. Man folgere hieraus, dass f_{mn} durch f_m teilbar ist.

(iii) $f_n f_{n+2} - (f_{n+1})^2 = (-1)^{n+1}$.

Tipp: Aufgabe 18.

Die folgenden Aufgaben sind für **Donnerstag, den 20.09.,** vorzubereiten:

Aufgabe 22: Für $n \in \mathbb{N}_+$ bezeichne $\varphi(n)$ die Anzahl derjenigen Zahlen $m \in \{1, 2, \ldots, n\}$ mit $\mathrm{ggT}(n, m) = 1$. Also $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \ldots$. Man bezeichnet φ als die Eulersche Phi-Funktion.
Es seien nun p und q Primzahlen, $p \neq q$, und $n := pq$.

(i) Beweisen Sie direkt (d.h. nur unter Benutzung der Definition, ohne weitere Resultate aus der Vorlesung zu benutzen):

$$\varphi(n) = (p-1)(q-1).$$

(ii) Zeigen Sie, dass n leicht faktorisiert werden kann, wenn $\varphi(n)$ bekannt ist.
Tipp: Sazu von Vieta.

(iii) Man faktorisiere (ohne Computer/Taschenrechner und unter Angabe alle Zwischenrechnungen) $n = 36114289$. Es ist $\varphi(n) = 36102256$.

Aufgabe 23:

(i) Es sei n eine beliebige natürliche Zahl, welche größer als 2 ist. Beweisen Sie, dass $\varphi(n)$ gerade ist.

(ii) Es seien $p = 11, q = 13$ und $n = pq$. Bestimmen Sie $\varphi(n)$, ein $e > 3$ mit $\mathrm{ggt}(e, \varphi(n)) = 1$ und ein d mit $ed \equiv 1 \pmod{\varphi(n)}$. Verschlüsseln Sie nun die „Nachricht“ $x = 17$ gemäß dem RSA-Algorithmus.

Aufgabe 24: Sei $m \in \mathbb{N}$, $m \neq 0$ und für $n \in \mathbb{N}$ sei $[n]$ der Rest der Division von n durch m (und nicht die Ihnen vielleicht vertraute Gaußklammer!!). Sei $k = \sum_{n=0}^{r} \varepsilon_n 2^n$ mit $\varepsilon_n \in \{0, 1\}$. Sei $a \in \mathbb{N}$, und seien $f(n)$ und $g(n)$ rekursiv definiert durch

$$\begin{aligned} g(0) := [a] \quad &, \quad f(0) := g(0)^{\varepsilon_0} \\ g(n+1) \quad &:= \quad [g(n)^2] \\ f(n+1) \quad &:= \quad [f(n) g(n+1)^{\varepsilon_{n+1}}] \end{aligned}$$

Beweisen Sie, dass $f(r) = [a^k]$ gilt.

Bemerkung:
Mit dieser Methode lassen sich die beim RSA-Algorithmus zum Ver- und Entschlüsseln benötigten Reste von Potenzen schnell berechnen.