Prof. Dr. U. Görtz **Sommersemester 2011**
Dr. U. Terstiege
A. Herrmann

Lineare Algebra II

3. Übungsblatt

Abgabe: Mittwoch, 27. April 2011 vor der Vorlesung (Postfach 7 in T03 R03).

Hausaufgabe 1

Bestimme die kleinste positive ganze Zahl, die bei der Teilung durch $2, 3, 4, 5$ und 6 jeweils den Rest 1 läßt und außerdem durch 7 teilbar ist. (Diese Aufgabe stammt aus Fibonaccis (ca. 1170 – ca. 1250) *Liber Abbaci*.)

Hausaufgabe 2

Beweise den Satz von Wilson: Ist p eine Primzahl, so ist $(p-1)! \equiv -1 \mod p$. Dabei ist $(p-1)!$ wie üblich definiert als das Produkt $1 \cdot 2 \cdot ... \cdot (p-1)$.
Anleitung: Zeige zunächst, daß es zu jedem $a \in \{1, ..., p-1\}$ ein eindeutig bestimmtes $b \in \{1, ..., p-1\}$ mit $a \cdot b \equiv 1 \mod p$ gibt. (Die Ergebnisse von Blatt 3 aus LA1 dürfen verwendet werden.) Zeige weiter, daß $b \neq a$, falls $a \neq 1, p-1$. Folgere, daß $(p-2)! \equiv 1 \mod p$ und damit $(p-1)! \equiv -1 \mod p$ gilt.

Hausaufgabe 3

a) Zeige: Ist p eine Primzahl, die kein Primelement in $\mathbb{Z}[i]$ ist, so ist p die Summe zweier Quadratzahlen.
Anleitung: Sei p eine solche Primzahl. Nach Voraussetzung gibt es $\alpha, \beta \in \mathbb{Z}[i]$, die beide keine Einheiten in $\mathbb{Z}[i]$ sind, mit $p = \alpha \cdot \beta$. Betrachte wieder die Normabbildung $N : \mathbb{Z}[i] \to \mathbb{N}$ wie auf Blatt 2 (also $N(x+iy) = x^2 + y^2$). Folgere, daß $p^2 = N(\alpha) \cdot N(\beta)$, und begründe nun, daß $N(\alpha) = N(\beta) = p$ gilt. Folgere daraus die Behauptung.

b) Sei p eine Primzahl der Form $p = 4n + 1$ für eine natürliche Zahl n. Zeige, daß p die Summe zweier Quadratzahlen ist. (Z.B. ist $73 = 4 \cdot 18 + 1 = 8^2 + 3^2$.)
Anleitung: Nach Teil a) genügt es zu zeigen, daß p kein Primelement in $\mathbb{Z}[i]$ ist. Sei $x = (2n)!$. Nutze den Satz von Wilson (Aufgabe 2), um zu zeigen, daß $x^2 \equiv -1 \mod p$ ist. Begründe nun: Wäre p ein Primelement in $\mathbb{Z}[i]$, so wäre p ein Teiler von $x + i$ oder $x - i$. Folgere daraus die Behauptung.

c) Sei nun p eine Primzahl der Form $p = 4n + 3$ für eine natürliche Zahl n. Zeige, daß p ein Primelement in $\mathbb{Z}[i]$ ist.
Anleitung: Untersuche, welche Reste die Summe zweier Quadratzahlen bei der Teilung durch 4 lassen kann, und nutze wieder das Kriterium aus Teil a).

Hausaufgabe 4: Beweise zum Thema Primzahlen in der Schule

18. *Anzahl der Primzahlen*

a) Die Primzahlen sind nicht regelmäßig verteilt. Die folgende Tabelle gibt einen Überblick über die Anzahl der Primzahlen. Ergänze die beiden ersten Angaben.

1 bis 100: □	1 bis 1000: 168	20000 bis 21000: 98
100 bis 200: □	1000 bis 2000: 135	30000 bis 31000: 95
900 bis 1000: 14	9000 bis 10000: 112	40000 bis 41000: 88

Die Primzahlen werden also immer seltener; man könnte vermuten, dass sie irgendwann einmal aussterben. Das ist aber nicht der Fall, denn es gibt unendlich viele Primzahlen.

b) (1) Berechne $2 \cdot 3 + 1$; $2 \cdot 3 \cdot 5 + 1$; $2 \cdot 3 \cdot 5 \cdot 7 + 1$; $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1$.

(2) Zeige, dass die nächste auf diese Weise gebildete Zahl $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1$ keine Primzahl ist.
Anleitung: Prüfe, ob die Zahl durch 37 oder 59 teilbar ist.

(3) Begründe: Die Zahl $2 \cdot 3 \cdot 5 \cdot \ldots \cdot p + 1$ ist entweder selbst eine Primzahl oder sie hat als Teiler eine Primzahl, die größer als die „letzte" Primzahl p ist.

(4) Anke überlegt nun: „Wenn jemand behauptet, es sei p die letzte aller Primzahlen, dann bildet man die Zahl $2 \cdot 3 \cdot 5 \cdot \ldots \cdot p + 1$ und erhält eine größere Primzahl oder einen größeren Primfaktor."

Abbildung 1: aus: Elemente der Mathematik Klasse 6 (Schrödel Verlag)

a) Lösen Sie die Aufgaben (1)-(3) in der Schulaufgabe 18 b).

b) Beweisen Sie die Aussage: Es gibt unendlich viele Primzahlen in $\mathbb{N}$.

Zusatzaufgabe:

Informieren Sie sich über das Sieb des Eratosthenes. Lösen Sie damit auch 18 a) der Schulaufgabe. Überlegen Sie sich weiterhin, warum es bei dem Verfahren genügt, die Vielfachen der Zahlen 1 bis 7 zu streichen, um alle Primzahlen zwischen 1 und 100 zu erhalten. Die Vielfachen welcher Zahlen genügt es zu streichen, um die Primzahlen zwischen 1 und 200 zu erhalten? Begründen Sie Ihre Antworten! Erkennen Sie eine Regel, von welchen Zahlen es genügt die Vielfachen zu streichen, um alle Primzahlen zwischen 1 und n ($n \in \mathbb{N}$ beliebig, aber fest) zu erhalten? Begründen Sie die Gültigkeit der von Ihnen aufgestellten Regel!