Mathematik I, Logik und Algebra, WS2010/11
M. Hortmann

Blatt 6

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen							Gruppe	Tutor
1a	2a	b	3a	3b	4	5	**Summe**	**bearbeitet**
1	1	1	1	1	1	1	6 Punkte=100%	

Euklidischer Algorithmus:
Sind $a, b \in \mathbb{N}$, so setze man $r_0 := a$, $r_1 := b$ und erzeuge rekursiv eine endliche Folge (r_i) durch Divisionen mit Rest: $r_{i-1} = q_i r_i + r_{i+1}$, $0 \leqslant r_{i+1} < r_i$. Schließlich wird $r_{i+1} = 0$. Dann: $r_i = \mathrm{ggT}(a, b)$.

Aufgabe 1:
a) Es sei a=2528976880919149, b=973327984803263. Berechnen Sie mit Hilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler von a und b.[1]
b) Freiwillige Sonderaufgabe: Schreiben Sie eine Pari-Funktion ggT(a,b)[2].

Aufgabe 2
a) Schreiben Sie das Sieb des Eratosthenes soweit hin, daß Sie alle Primzahlen zwischen 2 und 300 erhalten. (Beim Aussieben muß man nur nur bis zu den Vielfachen von 17 gehen. Warum?)

b) Die Primfaktorzerlegung von 260797 enthält nur Primzahlen unterhalb von 30. Wie sieht diese Zerlegung aus? Dokumentieren Sie alle Rechenschritte, die Sie zum Auffinden des Resultats führen.

c) Freiwillige Sonderaufgabe: Schreiben Sie eine Parifunktion Eratosthenes(n), welche das Sieb realisiert. Diese Funktion soll berechnen: die Anzahl der Primzahlen zwischen 2 und n, sowie die größte Primzahl unterhalb von n. Dokumentieren Sie die Rechenzeiten für wachsendes n.

---

1 d.h. konstruieren Sie die Folge (r_i) bis sich $r_{i+1} = 0$ ergibt. Die einzelnen Divisionsschritte dürfen mit Hilfe eines Arithmetik- oder Computeralgebraprogramms wie bc oder Pari durchgeführt werden, jedoch sind sämtliche Reste r_i zu dokumentieren, ebenso die Computerbefehle. Im vorliegenden Fall sind 23 Divisionsschritte durchzuführen.

2 Natürlich soll man nicht die eingebaute Pari-Funktion gcd verwenden.

Aufgabe 3
a) Es ist $60 = 2^2 \cdot 3 \cdot 5$. Benutzen Sie diese Primfaktorzerlegung, um alle positiven Teiler von 60 systematisch hinzuschreiben.

b) Die Zahl $n \in \mathbb{N}$ besitze die eindeutige Primfaktorzerlegung $\prod_{i=1}^{k} p_i^{\alpha_i}$. Begründen Sie, warum n $\prod_{i=1}^{k} (\alpha_i + 1)$ positive Teiler besitzt.

Es gilt: teilt eine Primzahl ein Produkt, so teilt sie einen der Faktoren. Außerdem gilt: Sind $a, b, c \in \mathbb{Z}$ und ist $c \neq 0$, so folgt $a=b$ aus $ac=bc$. Benutzen Sie dies, um zu zeigen:

Aufgabe 4
Sind $p_1 \leqslant p_2$ und $q_1 \leqslant q_2 \leqslant q_3$ positive Primzahlen, so ist $p_1 p_2 \neq q_1 q_2 q_3$ und aus $p_1 p_2 = q_1 q_2$ folgt $p_1 = q_1$ und $p_2 = q_2$.

Eine Variante des Induktionsprinzips funktioniert so:

Man möchte zeigen, daß $\forall n \in \mathbb{N}: \ E(n)$.
Man betrachte nun die Eigenschaft $F(n): \Leftrightarrow \ \forall m \in \mathbb{N}: \ (m \leqslant n \rightarrow E(m))$
Offenbar sind $\forall n \in \mathbb{N}: \ E(n)$ und $\forall n \in \mathbb{N}: F(n)$ äquivalent. Es könnte aber günstiger sein, einen Induktionsbeweis für $\forall n \in \mathbb{N}: F(n)$ zu führen. Der Vorteil gegenüber einem unmittelbaren Induktionsbeweis für $\forall n \in \mathbb{N}: \ E(n)$ liegt potentiell darin, daß die Induktionsvoraussetzung nun lautet $\forall m \in \mathbb{N}: \ (m \leqslant n \rightarrow E(m))$, d.h. man darf beim Induktionsschluß nicht nur die Gültigkeit von $E(n)$ voraussetzen, sondern zusätzlich die Gültigkeit von $E(m)$ für alle kleineren Elemente.

Aufgabe 5:
Sei jetzt $E(n)$ die folgende Eigenschaft:
$n=1$ oder es gibt ein $k \in \mathbb{N}$ und Primzahlen $p_1, \ldots, p_k$, so daß $n = p_1 \cdots p_k$.

Zeigen Sie mittels obiger Methode, daß $\forall n \in \mathbb{N}: \ E(n)$.

Damit haben Sie einen Beweis für die Existenz einer Primfaktorzerlegung für jede natürliche Zahl größer als 1.