# 12. Übungsblatt zu Mathematik für Informatiker II, SS 2004

JOACHIM VON ZUR GATHEN & MICHAEL NÜSKEN

Abgabe bis Montag, 26. Juli 2004, $12^{23}$ Uhr
in den jeweils richtigen Kasten auf dem D1-Flur.

**Aufgabe 12.1** (Reihen). (4+2 Punkte)

Zeige, dass die folgenden Reihen absolut konvergieren:

(i) $\displaystyle\sum_{k=1}^{\infty} \frac{1}{k^4 + z^4}$ für $z \in \mathbb{R}$.

(ii) $\displaystyle\sum_{k=1}^{\infty} k^{-2} \cos(kz)$ für $z \in \mathbb{R}$.

Zusatz: Zeichne (mit Hilfe von MuPAD oder Maple) für beide Reihen den Graphen der Partialsummen bis $k = 1, 2, 3, 4, 5, 10, 20, 50$ im Intervall $[-5, 5]$. *Hilfe:* In MuPAD 3.0 kann man mit

```
X1:=plot::Function2d( sum(k^(2)*exp(-k*z),k=1..2), z=-5..5,
                Color=RGB::Blue ):
X2:=plot::Function2d( sum(k^(2)*exp(-k*z),k=1..5), z=-5..5,
                Color=RGB::Red ):
plot(X1,X2,ViewingBoxYRange=-1..40);
```

und in Maple mit

```
X1:=plot( sum(k^{2}*exp(-k*z),k=1..2), z=-5..5,
          color=blue ):
X2:=plot( sum(k^{2}*exp(-k*z),k=1..5), z=-5..5,
          color=red ):
plots[display](X1,X2);
```

ein Bild mehrer Graphen gleichzeitig zeichnen.

**Aufgabe 12.2** (Konvergenzradius). (4 Punkte)

Bestimme den Konvergenzradius folgender Potenzreihen.

(i) $\displaystyle\sum_{n=1}^{\infty} \left(\frac{z}{n}\right)^n$.

(ii) $\displaystyle\sum_{n=3}^{\infty} \frac{z^n}{n(\log n)^n}$.

(iii) $\sum_{n=0}^{\infty}(n+1)z^n$.

(iv) $\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}z^n$.

*Lexikon:* $\lim_{n\to\infty}\sqrt[n]{n}=1$.

**Aufgabe 12.3** ($\Omega$). (5 Punkte)

Wir definieren $\Omega(1)$ als die Menge aller reellen Folgen $(a_n)_{n\in\mathbb{N}}$ für die es eine Konstante $C\in\mathbb{R}_{>0}$ gibt mit $|a_n|\geq C$ für alle $n$;

$$\Omega(1)=\left\{a\in\mathbb{R}^{\mathbb{N}}\;\middle|\;\exists C>0\colon\forall n\in\mathbb{N}\colon\ |a_n|\geq C\right\}.$$

Damit bedeutet $a\in\Omega(b):=\Omega(1)\cdot b$, dass $\left(\frac{a_n}{b_n}\right)_{n\in\mathbb{N}}\in\Omega(1)$ liegt, also von der Null weg beschränkt ist. Prüfe (und begründe):

(i) $n^4\in\mathcal{O}(n^5)$.

(ii) $\frac{1}{42}n^3-n\in\mathcal{O}(n^3)$.

(iii) $\frac{3^n}{n^2}-n^{17}\in\mathcal{O}(2^n)$.

(iv) $n\log n\operatorname{loglog} n\in\mathcal{O}(n^2)$.

(v) $\frac{n}{\log n}\in\mathcal{O}(\sqrt{n})$.

(vi) $n^4\in\Omega(n^5)$.

(vii) $\frac{1}{42}n^3-n\in\Omega(n^3)$.

(viii) $\frac{3^n}{n^2}-n^{17}\in\Omega(2^n)$.

(ix) $n\log n\operatorname{loglog} n\in\Omega(n^2)$.

(x) $\frac{n}{\log n}\in\Omega(\sqrt{n})$.

**Aufgabe 12.4** (Quotientenkriterium). (4 Punkte)

Beweise das Quotientenkriterium in der folgenden „Vollversion“:

**Satz** (Quotientenkriterium). *Sei $\sum_{n=0}^{\infty}a_n$ eine Reihe mit $a_n\neq 0$ für alle $n\geq 0$. Es gebe eine reelle Zahl $q$ mit $0<q<1$ so, dass*

$$\left|\frac{a_{n+1}}{a_n}\right|\leq q$$

*für alle $n\geq N$. Dann konvergiert die Reihe $\sum_{n=0}^{\infty}a_n$ absolut (und damit auch gewöhnlich).*

***Aufgabe 12.5** (Crossover). (4 Punkte)

Es gibt Algorithmen zur Faktorisierung von natürlichen Zahlen mit ganz unterschiedlichen Laufzeiten. MuPad 3.0 hat die Funktionen `numlib::pollard`, `numlib::ecm` mit den Laufzeiten $\mathcal{O}^{\sim}(2^{n/4})$, $\mathcal{O}^{\sim}(2^{\sqrt{n}})$. Wir haben noch die Prozedur `triv_ifactor` beigesteuert, die mit der trivialen Methode einen

Faktor findet. Ihre Laufzeit beträgt $\mathcal{O}(2^{n/2})$. [MuPADs Funktion `ifactor` verwendet eine Kombination verschiedener Techniken, ua. eine Tabelle der Primzahlen bis $300\,000$ und `numlib::ecm`. Sie ist damit asymptotisch gleich schnell wie `numlib::ecm`.] Wir haben Messung vorgenommen auf einem 700MHz-Pentium-III-Rechner, unter anderem mit einer 48-Bitzahl, die ein Produkt zweier 24-Bitzahlen war und folgende Laufzeiten gemessen:

| Algorithmus<br>Schranke | `triv_ifactor`<br>$\mathcal{O}(2^{n/2})$ | `numlib::pollard`<br>$\mathcal{O}^{\sim}(2^{n/4})$ | `numlib::ecm`<br>$\mathcal{O}^{\sim}(2^{\sqrt{n}})$ | `ifactor`<br>$\mathcal{O}^{\sim}(2^{\sqrt{n}})$ |
|---|---|---|---|---|
| Messung 40-Bit | 4,226 sec | 0,050 sec | 0,231 sec | 0,040 sec |
| Messung 48-Bit | 46,717 sec | 0,100 sec | 0,150 sec | 0,050 sec |

Nimm an, dass die Schranken „exakt“ sind. [Also etwa, dass die Laufzeit des trivialen Algorithmus *gleich* $c \cdot 2^{n/2}$ ist mit einer gewissen Konstante $c$.] Untersuche die drei Algorithmen `triv_ifactor`, `numlib::pollard` und `numlib::ecm`.

(i*) Bestimme anhand der Messung mit 48-Bit-Eingabe jeweils die Konstante.

(ii*) Bestimme die Bitlänge $n$ der Zahlen, die mit demselben Rechner innerhalb eines Tages faktorisierbar wären.

(iii*) Bestimme die Bitlänge $n$ der Zahlen, die mit 1000 10-GHz-Rechnern innerhalb eines Tages faktorisierbar wären.

(iv*) Für welche Bitlängen ist welcher Algorithmus der schnellste? [Bestimme hierzu die Crossoverpunkte, dh. die Bitlängen, wo die Algorithmen einander in der Geschwindigkeit ablösen.]

```
triv_ifactor:=proc(n)
begin
  if n mod 2=0 then return(2); end_if;
  for k from 3 to floor(sqrt(n)) step 2 do
    if n mod k=0 then return(k); end_if;
  end_for;
  return(n);
end_proc:
```

# 12. Übungsblatt zu Mathematik für Informatiker II, SS 2004, Mündlicher Teil

JOACHIM VON ZUR GATHEN & MICHAEL NÜSKEN

**Mündliche Aufgabe 12.6** (Reihen).

Zeige, dass die folgenden Reihen absolut konvergieren:

(i) $\displaystyle\sum_{k=1}^{\infty} \frac{1}{k^2+z^2}$ für $z \in \mathbb{R}$.

(ii) $\displaystyle\sum_{k=1}^{\infty} k^2\, \mathrm{e}^{-kz}$ für $z \in \mathbb{R}_{>0}$.

**Mündliche Aufgabe 12.7** (Konvergenzradius).

Bestimme den Konvergenzradius folgender Potenzreihen.

(i) $\displaystyle\sum_{n=1}^{\infty} \left(\frac{z}{\log n}\right)^n$.

(ii) $\displaystyle\sum_{n=3}^{\infty} \frac{z^n}{n(\log\log n)^n}$.

(iii) $\displaystyle\sum_{n=0}^{\infty} (n+2)(n+1)z^n$.

(iv) $\displaystyle\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} z^n$.

*Lexikon:* $\lim\limits_{n\to\infty} \sqrt[n]{n} = 1$.

**Mündliche Aufgabe 12.8** ($2^{\mathcal{O}}$).

Prüfe und begründe:

(i) $f \in \mathcal{O}(g) \;\Rightarrow\; 2^f \in \mathcal{O}(2^g)$.

(ii) $f \in \mathcal{O}(g) \;\Rightarrow\; 2^f \in 2^{\mathcal{O}(g)}$.

Für eine Menge $X \subset \mathbb{R}^{\mathbb{N}}$ von Folgen bedeutet die Notation $2^X$ die Menge aller Folgen $(2^{a_n})_{n\in\mathbb{N}}$ mit $a \in X$;

$$2^X = \{2^a \mid a \in X\}.$$

Eigentlich sollte man stattdessen $\mathcal{O}(1) \cdot 2^X$ nehmen. Warum?

**Mündliche Aufgabe 12.9** (Majorantenkriterium).

Beweise das Majorantenkriterium in der folgenden „Vollversion“:

**Satz** (Majorantenkriterium). *Sei $\sum_{n=0}^{\infty} b_n$ eine konvergente Reihe mit $b_n \geq 0$ für alle $n \geq 0$, $c \in \mathbb{R}_{>0}$ und $(a_n)_{n\in\mathbb{N}}$ eine Folge mit $|a_n| \leq c b_n$ für alle $n \in \mathbb{N}$. Dann konvergiert die Reihe $\sum_{n=0}^{\infty} a_n$ absolut (und damit auch gewöhnlich).*