

Übungsblatt 7

Besprechung am 2.12.2010

Aufgabe 1 Um das Kryptosystem RSA zu knacken, müssen sehr große Zahlen faktorisiert werden. Die Tabelle enthält Daten eines Experiments, bei dem relativ (!) kleine Zahlen faktorisiert wurden: x_i ist die Anzahl der Dezimalstellen und t_i die dafür benötigte Rechenzeit in Sekunden.

x_i	41	43	46	47	50	52	54	56
t_i	0.7	1.3	3.9	5.2	18.1	26.8	36.7	68.2
$y_i = \log(t_i)$	-0.34	0.28	1.36	1.64	2.89	3.29	3.60	4.22

Der lineare Zusammenhang zwischen x_i und y_i soll mittels linearer Regression modelliert werden. Verwenden Sie dazu, dass die allgemeine Regressionsgerade $y = kx + d$ immer durch den Schwerpunkt $(\frac{1}{n} \sum_i x_i, \frac{1}{n} \sum_i y_i)$ verläuft. Verschieben Sie die Daten entsprechend und berechnen Sie die Steigung der Regressionsgerade durch den Ursprung. Nutzen Sie diese, um abzuschätzen, wie lange der Computer des Experiments brauchen würde, um einen 4096-Bit-Schlüssel (also eine Binärzahl mit 4096 Stellen – wie viele Dezimalstellen sind das?) zu knacken.

Aufgabe 2 Berechnen Sie die folgenden unbestimmten Integrale:

a) $\int \sin(x)\sqrt{\cos(x)} dx$ b) $\int \sin(x)e^x dx$ c) $\int x^3 e^{x^2} dx$ d) $\int \frac{1}{e^x + 1} dx$

Aufgabe 3 Berechnen Sie das bestimmte Integral

$$\int_0^{1/2} \frac{3x^2 - 2x + 3}{x^4 - 1} dx,$$

indem Sie zunächst $a, b, c, d \in \mathbb{R}$ bestimmen, so dass

$$\frac{3x^2 - 2x + 3}{x^4 - 1} = \frac{a}{x + 1} + \frac{b}{x - 1} + \frac{cx + d}{x^2 + 1}$$

die Partialbruchzerlegung des Integranden ist. Integrieren Sie dann termweise!

Aufgabe 4 Uneigentliche Integrale

Ein Integral heißt “uneigentlich”, wenn der Integrationsbereich unbeschränkt ist oder wenn die zu integrierende Funktion innerhalb des Integrationsbereiches unbeschränkt ist.

a) Zeigen Sie, dass das uneigentliche Integral

$$\int_0^1 \frac{1}{x^2} dx := \lim_{a \rightarrow 0^+} \int_a^1 \frac{1}{x^2} dx$$

nicht konvergiert, indem Sie eine Abschätzung mittels Riemannsummen vornehmen!

b) Zeigen Sie erneut, dass die harmonische Reihe nicht konvergiert, indem Sie sie mit einem uneigentlichen Integral der Form

$$\int_1^\infty f(x) dx := \lim_{a \rightarrow \infty} \int_1^a f(x) dx$$

abschätzen!

Aufgabe 5 Programmieren Sie eine Funktion in Sage, die zu einer gegebenen Funktion $f(x)$ und einem Intervall $[a, b]$ einen Näherungswert für das Integral $\int_a^b f(x) dx$ berechnet.