Übungsblatt 1 für Analyse von Algorithmen (10.10.2012)

1.) Man führe Mergesort vollständig für die Liste $4, 6, 2, 1, 3, 5$ durch. (Man verwende dabei den in der Vorlesung ausgeteilten Algorithmus und ziehe die Schritte einzeln nach.)

2.) Man formuliere (und formalisiere) einen Sortiertalgorithmus, wo zunächst (mit Hilfe von Vergleichsoperationen) das kleinste Element gesucht wird etc. Welches *worst-case*-Verhalten wird dieser Algorithmus haben? (Begründung!)

3.) Man zeige, dass die *divide and conquer*-Rekursion

$$C_N = C_{\lceil N/2 \rceil} + C_{\lfloor N/2 \rfloor} + N, \quad N \geq 2, \quad C_1 = 0,$$

die explizite Lösung

$$C_N = N\lceil \log_2 N \rceil + N - 2^{\lceil \log_2 N \rceil}$$

hat.

4.) Man zeige, dass im Fall $\alpha = \log a / \log b < c$ die Lösung der *divide and conquer*-Rekursion $T(x) = aT(x/b) + O(x^c)$ $(x \geq b)$ die obere Abschätzung $T(x) = O(x^c)$ erfüllt.
($T(x)$ ist positiv und für $x \geq 1$ definiert und im Intervall $[1, b]$ beschränkt; $a, c > 0$, $b > 1$.)

5.) Entsprechend zeige man im Fall $\alpha = c$ die Abschätzung $T(x) = O(x^c \log x)$.

Übungsblatt 2 für Analyse von Algorithmen (17.10.2012)

6.) Man zeige folgende Eigenschaft: Sei $g(x)$, $x \geq 1$, eine Riemann-integrierbare Funktion mit der Eigenschaft, dass es Konstanten $c_1, c_2 > 0$ gibt, so dass

$$c_1 g(x) \leq g(u) \leq c_2 g(x) \qquad \text{für } x \geq 1/b \text{ und für alle } u \text{ mit } bx \leq u \leq x,$$

für ein b mit $0 < b < 1$ gilt. Dann gibt es für jede reelle Zahl α Konstanten $c_3, c_4 > 0$ mit

$$c_3 g(x) \leq x^\alpha \int_{bx}^{x} \frac{g(u)}{u^{\alpha+1}}\, du \leq c_4 g(x) \qquad \text{für alle } x \geq 1/b.$$

7.) Man formuliere eine diskrete Version des Satzes von Akra-Bazzi.

8.) Der **Karatsuba-Algorithmus** zur Multiplikation zweier ganzer Zahlen $x = (x_n \cdots x_1)_2$, $y = (y_n \cdots y_1)_2$ (im Binärsystem) basiert auf folgender Idee. Man schreibt x und y in der Form $x = x' + 2^m x''$ und $y = y' + 2^m y''$ mit $m = \lfloor n/2 \rfloor$. und berechnet $A = x'y'$, $B = x''y''$ und $C = (x' + x'')(y' + y'')$. Dann gilt

$$x \cdot y = A + 2^m(C - A - B) + 2^{2m} B.$$

Man gebe eine obere Abschätzung für den Aufwand des Karatsuba-Algorithmus an, wobei der Aufwand in der Anzahl der elementarem Rechenoperationen (von 0 und 1) berechnet werden soll?

9.) Wie ist das asymptotische Verhalten der Lösung der Divide-and-Conquer-Rekursion

$$T(x) = 2T(x/2) + \frac{8}{9} T(3x/4) + \Theta(x^2/\log x) \quad ?$$

10.) Wie ist das asymptotische Verhalten der Lösung der Divide-and-Conquer-Rekursion

$$T(x) = 2T(x/4) + 3T(x/6) + \Theta(x \log x/\log\log x) \quad ?$$

Übungsblatt 3 für Analyse von Algorithmen (24.10.2012)

11.) Sei

$$G(z) = \mathbb{E}(z^X) = \frac{1}{n}\frac{z^{n+1} - z}{z - 1}$$

die wahrscheinlichkeitserzeugende Funktion der Zufallsvariablen X. Man berechne den Erwartungswert und die Varianz von X.
(Die Regel von l'Hospital ist hier eher unpraktisch...)

12.) Zu einer Zufallsvaraiblen X mir wahrscheinlichkeitserzeugenden Funktion $F(z) = \mathbb{E}(z^X) = \sum_{k\geq 0} p_k z^k$ (mit $p_k = \mathbb{P}[X = k]$) sei $M_s = \sum_{k\geq 0} k^s p_k = \mathbb{E}(X^s)$ das s-te Moment. (M_1 ... Erwartungswert, $M_2 - M_1^2$ ... Varianz.) Weiters bezeichne $\xi = \xi(X) = M_3 - 3M_2M_1 + 2M_1^3$. Man zeige für zwei unabhängige Zufallsvariable X und Y:

$$\xi(X + Y) = \xi(X) + \xi(Y).$$

Wie kann $\xi(X)$ (ähnlich wie die Varianz) gedeutet werden?

13.) Berechnen Sie

$$[z^n u^j]\frac{1}{(1 - zu)(1 - z)} \log \frac{1}{1 - zu} \quad \text{und} \quad [z^n u^j]\frac{1}{(1 - zu)(1 - z)} \log \frac{1}{1 - z}\,.$$

Anmerkung: für eine Potenzreihe $F(z) = \sum_{n\geq 0} F_n z^n$ bezeichnet $[z^n]F(z)$ den Koeffizienten von z^n in $F(z)$, also: $[z^n]F(z) = F_n$.

14.) Man behandle die Quicksort-Rekursion für den Erwartungswert der Anzahl der Vergleichsoperationen mit Hilfe einer Differentialgleichung:

(a) Aus

$$nC_n = n(n - 1) + 2\sum_{k=0}^{n-1} C_k\,, \quad C_0 = C_1 = 0\,, \quad C(x) = \sum_{k\geq 0} C_k z^x$$

schließe man

$$C'(x) = \frac{2}{1 - x}C(x) + \frac{2z}{(1 - x)^3}\,.$$

(b) Man löse die Gleichung in a.) für $C(0) = 0$; $C'(0) = 0$ und lese daraus den Koeffizienten C_n ab.

15.) Man finde eine alternative Definition für die harmonischen Zahlen $H_n = 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$, die auch für komplexe Zahlen Sinn macht. Genauer: Man finde eine "sinnvolle" Funktion $H(x)$, sodaß $H_n = H(n)$.
Hinweis: Studiere $\sum_{k>0} \left(\frac{1}{k} - \frac{1}{n+k}\right)$.

Übungsblatt 4 für Analyse von Algorithmen (31.10.2012)

16.) Auffinden des j-größten Elements aus $x[1], \ldots, x[n]$. (Quickselect)

Anmerkung: Quickselect funktioniert nach dem Prinzip von Quicksort, d.h. in der Partitionierungsphase wird ein zufällig gewähltes Element durch Vergleiche mit den übrigen Elementen an die richtige Position gebracht, sodaßsich anschließend links vom Pivotelement nur Elemente kleiner und rechts vom Pivotelement nur Elemente größer als das Pivotelement befinden. Danach wird untesucht, ob das Pivotelement bereits das gesuchte Element darstellt und gegebenenfalls dieses zurückgegeben. Falls dies nicht der Fall ist, wird anschließend nur in einem Teilfeld, in dem sich das gesuchte Element befinden muß, rekursiv weitergesucht.

Begründen Sie für die mittlere Anzahl $D_{n,j}$ der rekursiven Aufrufe (= Durchläufe) von Quickselect die Rekursion

$$D_{n,j} = 1 + \frac{1}{n}\left(\sum_{k=1}^{j-1} D_{n-k,j-k} + \sum_{k=j+1}^{n} D_{k-1,j}\right) \quad \text{für } n \geq j \geq 1\,.$$

Setzen Sie sodann $D_{n,j} = H_j + H_{n+1-j} - 1$ ein und sehen Sie, daß die Formel stimmt.

17.) Die mittlere Anzahl $C_{n,j}$ der Vergleiche bei Quickselect ist durch folgende Formel gegeben (brauchen Sie nicht zeigen):

$$C_{n,j} = 2\left[(n+1)H_n - (n+3-j)H_{n+1-j} - (j+2)H_j + n + 3\right]\,.$$

Auffinden des Medians: Setze $n = 2N + 1$, $j = N + 1$. Bestimmen Sie das asymptotische Verhalten für $N \to \infty$.

18.) Gegeben sei die folgende Inversionstafel von $\pi : (4, 2, 3, 0, 1, 0, 1, 0, 0)$. Geben Sie die kanonische Zyklendarstellung von π an.

19.) Skizzieren Sie einen Algorithmus, um aus einer Inversionstafel zur entsprechenden Permutation zu gelangen. (Abarbeitung der Inversionstafel von vorne.)

20.) $I_n(k)$ sei die Anzahl der Permutationen von $\{1, \ldots, n\}$ mit k Inversionen. Zeigen Sie:

$$I_n(k) = I_n(k-1) + I_{n-1}(k) \quad \text{für } k < n,$$

$$\sum_k I_n(k) = n!,$$

$$\sum_k I_n(k) z^k = \prod_{k=0}^{n-1} (1 + \cdots + z^k),$$

$$\sum_k (-1)^k I_n(k) = 0, \quad n \geq 2,$$

$$\sum_k k I_n(k) = \frac{1}{2} \binom{n}{2} n!.$$

Übungsblatt 5 für Analyse von Algorithmen (7.11.2012)

21.) Bei der Analyse von Hashing mit Linear Probing trat folgende Summe auf (mit $n \in \mathbb{N}$):

$$S(n,x,y) := (y-n)\sum_{k=0}^{n}\binom{n}{k}(x+k)^{k+1}(y-k)^{n-k-1}.$$

Man zeige nun folgende Rekursion für $S(n,x,y)$:

$$S(n,x,y) = x(x+y)^n + nS(n-1,x+1,y-1), \text{ für } n \geq 1, \quad S(0,x,y) = x.$$

Daraus folgere man:

$$S(n,x,y) = \sum_{k=0}^{n}(x+k)n^{\underline{k}}(x+y)^{n-k}.$$

Anmerkung: Abels's Verallgemeinerung des Binomischen Lehrsatzes erweist sich als nützlich.

22.) Ramanujan's Q-Funktion sei definiert durch

$$Q(n) := \sum_{k\geq 0}\frac{(n-1)^{\underline{k}}}{n^k}\,.$$

Man zeige für natürliche Zahlen n:

$$1 + Q(n) = \int_0^\infty e^{-x}\left(1+\frac{x}{n}\right)^n dx\,.$$

23.) Man betrachte

$$\tilde{Q}(m,n) = \sum_{k\geq 0}\frac{n^{\underline{k}}}{m^k}.$$

Man setze $n = \alpha m$, mit $0 < \alpha < 1$ und studiere das asymptotische Verhalten von $\tilde{Q}(m,\alpha m)$ für $m \to \infty$.
Anleitung: Zeigen (beispielsweise durch Induktion) und werwenden Sie

$$n^k - \binom{k}{2}n^{k-1} \leq n^{\underline{k}} \leq n^k.$$

24.) Alternative Herleitung von Abel's Verallgemeinerung des Binomischen Lehrsatzes

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x(x-kz)^{k-1}(y+kz)^{n-k}\,.$$

Anleitung: Definiere $a_0(x,z) = 1$, $a_k(x,z) = \frac{x(x-kz)^{k-1}}{k!}$ für $k \geq 1$.

(a) Zeige

$$\frac{\partial^j}{\partial x^j} a_k(x,z) = a_{k-j}(x - jz, z)\,.$$

(b) Man fasse z stets als Parameter auf. Jedes $P(x)$ lässt sich eindeutig schreiben als $P(x) = \lambda_0 a_0 + \cdots + \lambda_n a_n$. Man zeige nun

$$\lambda_j = P^{(j)}(jz)\,.$$

(c) Wende die Darstellung

$$P(x) = \sum_{k=0}^{n} P^{(k)}(kz) a_k(x,z)$$

auf das Polynom $(x+y)^n$ an.

25.) Zeige durch geeignete Wahl von $P(x)$:

$$a_n(x+y,z) = \sum_{k=0}^{n} a_k(x,z) a_{n-k}(y,z)\,.$$

Übungsblatt 6 für Analyse von Algorithmen (14.11.2012)

26.) Das Parkproblem: eine Einbahnstraße besitze m in einer Reihe angeordnete Parkplätze, die von 1 bis m numeriert sind. Ein Mann fährt mit seiner im Auto eingeschlafenen Frau die Einbahnstraße entlang, plötzlich wacht die Frau auf und weist den Mann an, ehestmöglich zu parken. Daraufhin versucht er an der ersten freien Stelle zu parken, aber falls kein freier Parkplatz mehr verfügbar ist (also wenn beim Aufwachen der Frau Platz k erreicht ist, aber $k, k+1, \ldots, m$ besetzt sind), beschließt er, nicht verkehrswidrig zu parken, sondern weiterzufahren. Wir nehmen nun an, dies geschieht für n verschiedene Autos, wobei die j-te Frau beim Parkplatz a_j aufwacht. Wie viele Folgen $a_1, a_2, \ldots, a_n \in \{1, \ldots, m\}^n$ gibt es dann, wo alle Autos geparkt werden können, unter der Voraussetzung, daß die Straße zu Beginn leer ist und keines der geparkten Autos wieder weggefahren wird?

Hinweis: es gibt einen einfachen Zusammenhang mit einer "Hilfsgröße", die bei der Analyse von Hashing mit Linear Probing studiert wurde.

27.) Betrachten Sie Binäre Suchbäume mit n gespeicherten Daten. Sei $P_{n,k}$ die Wahrscheinlichkeit, daß die letzte Eintragung k Schritte benötigt. Zeigen Sie:

(a) $\mathbb{E}C_{n-1}^{[\ell]} = \sum kP_{n,k}$ ($C_{n-1}^{[\ell]}$ ... Anzahl der Schritte bei der erfolglosen Suche)

(b) $nP_{n,k} = 2P_{n-1,k-1} + (n-2)P_{n-1,k}$

(c) Sei $P_n(z) = \sum_{k\geq 0} P_{n,k} z^k$. Zeigen Sie

$$P_n(z) = \prod_{2\leq j\leq n} \frac{2z+j-2}{j}\,.$$

Hieraus bestimme man Erwartungswert und Varianz.

28.) Beweisen Sie folgenden Zusammenhang zwischen der Internen Pfadlänge $I(t)$ und der Externen Pfadlänge $E(t)$ eines Binärbaums t:

$$E(t) = I(t) + 2|t|,$$

wobei Sie den Binärbaum bei der Wurzel in zwei (binäre) Teilbäume aufteilen und eine Induktion führen.

29.) Sei

$$f(z) = \frac{1-\sqrt{1-4z}}{2}.$$

Man betimme die Koeffizienten $[z^n]$ von $f(z)^r$, für $r \in \mathbb{N}$.

30.) Zur Pfadlänge in Tries: Lösen Sie (im Unterschied zur Vorlesung) die Funktionalgleichung

$$L(z) = z(e^z - 1) + 2e^{\frac{z}{2}} L(\frac{z}{2})$$

durch Iteration. Danach lesen Sie aus der Lösung die Koeffizienten ab und finden

$$L_n = n \sum_{k \geq 0} \left[1 - \left(1 - \frac{1}{2^k} \right)^{n-1} \right] .$$

Übungsblatt 7 für Analyse von Algorithmen (21.11.2012)

31.) Mittlere interne Pfadlänge in Digitalen Suchbäumen.

Wie bei Tries sind den Daten $0-1$-Folgen zugeordnet. Wie bei binären Suchbäumen werden die Daten der Reihe nach als interne Knoten eingetragen, wobei man, falls ein Knoten schon besetzt ist, nach links (0) bzw. rechts (1) verzweigt, und dafür fortlaufend die Bits verwendet.

(a) Man betrachte ein selbstgewähltes Beispiel mit 5 Daten und konstruiere den Digitalen Suchbaum.

(b) Zeigen Sie für die mittlere Interne Pfadlnge A_n von Digitalen Suchbumen mit $n \geq 1$ Daten:

$$A_n = n - 1 + \sum_{k=0}^{n-1} 2^{1-n} \binom{n-1}{k} (A_k + A_{n-1-k}) \,.$$

32.) Fortsetzung von Bsp. 31.):

(a) Sei

$$A(z) = \sum_{n \geq 0} A_n \frac{z^n}{n!} \,.$$

Zeige:

$$A'(z) = ze^z + 2e^{\frac{z}{2}} A(\frac{z}{2}) \,.$$

(b) Setze $B(z) = e^{-z} A(z)$. Zeige

$$B'(z) + B(z) = z + 2B(\frac{z}{2}) \,.$$

33.) Fortsetzung von Bsp. 32.):

(a) Sei

$$B(z) = \sum_{n \geq 0} B_n \frac{z^n}{n!} \,.$$

Zeige:

$$B_n = -(1 - 2^{2-n}) B_{n-1}, \quad \text{für } n \geq 3$$

bzw.

$$B_n = (-1)^n Q_{n-2} \quad \text{mit} \quad Q_n = \prod_{1 \leq j \leq n} \left(1 - \frac{1}{2^j}\right) \,.$$

(b) Daraus folgere man:

$$A_n = \sum_{k=2}^{n} \binom{n}{k} (-1)^k Q_{k-2}\,.$$

34.) Man zeige die ABELsche Umformung:

$$\sum_{1\le k\le N} a_k b_k = a_N \sum_{1\le k\le N} b_k - \sum_{1\le k<N} (a_{k+1} - a_k) \sum_{1\le i\le k} b_i$$

und mit deren Hilfe berechne man $\displaystyle\sum_{1\le k<n} \binom{k}{m} H_k$.

35.) Man zeige

$$[z^n] \frac{1}{(1-z)^{\alpha+1}} \log \frac{1}{1-z} = \binom{n+\alpha}{n} \left(H_{n+\alpha} - H_\alpha\right).$$

Übungsblatt 8 für Analyse von Algorithmen (28.11.2012)

36.) Sei $t \in \mathbb{Z}$ ein Parameter. Die gewöhnliche erzeugende Funktion $y(z)$ sei implizit definiert durch die Gleichung

$$y^{1-t} - y^{-t} = z\,.$$

Substituieren Sie

$$z = \frac{u}{(1+u)^t}$$

und zeigen Sie mit der Cauchy'schen Integralformel, dass für $r \in \mathbb{N}$

$$y^r = \sum_{k\geq 0} \binom{tk+r}{k} \frac{r}{tk+r} z^k\,.$$

und

$$\frac{y^r}{1-t+\frac{t}{y}} = \sum_{k\geq 0} \binom{tk+r}{k} z^k$$

gilt.

37.) Ein ebener Wurzelbaum besteht aus einem Wurzelknoten, wo eine Folge von beliebig vielen Unterbäumen (ergo, die links-rechts-Reihenfolge der Unterbäume ist wichtig), die selbst wiederum ebene Wurzelbäume sind, dranhängen.

(a) Wie viele ebenen Wurzelbäume mit n Knoten gibt es?

(b) Man interpretiere ebene Wurzelbäume als Gitterpfade, indem man, bei der Wurzel startend, um den Baum herumfährt und einen Abwärtsschritt als $\nearrow$ und einen Aufwärtsschritt als $\searrow$ zeichnet. Man betrachte ein repräsentatives Beispiel. Was haben diese Pfade für Eigenschaften?

(c) Man bestimme die Anzahl der Gitterpfade von $(0,0)$ nach $(2n,0)$, die nie unterhalb der x-Achse sind und die Anzahl der Gitterpfade von $(0,0)$ nach $(2n,0)$, die oberhalb der x-Achse sind und nur bei $(0,0)$ und $(2n,0)$ die x-Achse treffen.

38.) Sei $G(z)$ eine wahrscheinlichkeitserzeugende Funktion. Die sogenannten Semi-Invarianten oder Kumulanten κ_n, $n \geq 1$ sind definiert durch

$$\sum_{n\geq 1} \kappa_n \frac{t^n}{n!} = \ln G(e^t), \quad \text{also } \kappa_n = \frac{d^n}{dt^n} \ln G(e^t)\bigg|_{t=0}\,.$$

Es gilt also beispielsweise $\kappa_1 = G'(1)$, $\kappa_2 = G''(1) + G'(1) - \big(G'(1)\big)^2$.

Sei nun $F(z)$ definiert mittels $F(z) := z^m G(z)$ für ein beliebiges $m \in \mathbb{N}$ und bezeichne $\tilde{\kappa}_n$ die entsprechenden Semi-Invarianten. Welcher Zusammenhang besteht nun zwischen den κ_n und den $\tilde{\kappa}_n$?

39.) Falls für eine Diskrete Zufallsvariable X gilt, dass für alle $k \geq 0$: $\mathbb{P}\{X = k\} = \frac{e^{-\mu}\mu^k}{k!}$, dann heisst X Poisson-verteilt mit Parameter μ. Man berechne nun die wahrscheinlichkeitserzeugende Funktion $G(z) = \sum_{k\geq 0} \mathbb{P}\{X = k\} z^k$ und berechne weiters die im vorigen Bsp. definierten Semi-Invarianten κ_n.

40.) Zeigen Sie: Für $|k| \geq n^{\frac{1}{2}+\epsilon}$ gilt

$$\frac{\binom{2n}{n-k}}{\binom{2n}{n}} = \mathcal{O}\left(e^{-n^{2\epsilon}}\right) .$$

Dazu kann man beispielsweise die Beziehung

$$\frac{\binom{2n}{n-k}}{\binom{2n}{n}} = \frac{n(n-1)\cdots(n-k+1)}{(n+k)(n+k-1)\cdots(n+1)} = \left(1-\frac{k}{n+k}\right)\cdots\left(1-\frac{k}{n+1}\right) \leq \left(1-\frac{k}{n+k}\right)^k$$

benutzen.

Übungsblatt 9 für Analyse von Algorithmen (5.12.2012)

41.) Man zeige, dass die Riemannsche Zetafunktion $\zeta(s) = \sum_{k\geq 1} k^{-s}$ für $\Re(s) > 1$ konvergiert und zeige, dass sie in jedem Punkt s_0 mit $\Re(s_0) > 1$ eine konvergente Potenzreihenentwicklung

$$\zeta(s) = \sum_{n\geq 0} a_n (s - s_0)^n \qquad (|s - s_0| < R, \quad R = R(s_0) > 0)$$

besitzt.
Hinweis: Man entwickle k^{-s} zuerst in eine Potenzreihe.

42.) Man zeige für $\Re(s) > 1$ die Identität

$$\zeta(s) = \frac{s}{s-1} - s \int_1^\infty \frac{x - \lfloor x \rfloor}{x^{s+1}}\, dx.$$

Weiters zeige man, dass das Integral auf der rechten Seite eine Funkion in s darstellt, die für $\Re(s) > 0$ konvergiert und wieder in jedem Punkt s_0 mit $\Re(s_0) > 0$ eine konvergente Potenzreihenentwicklung besitzt.

43.) Es seien $A(s) = \sum_{k\geq 1} a_k k^{-s}$ und $B(s) = \sum_{k\geq 1} b_k k^{-s}$ zwei Dirichletsche Reihen mit Koeffizieten a_k bzw. b_k, die für $\Re(s) > \sigma_0$ absolut konvergieren. Für welche Koeffizienten c_k ist das Produkt $C(s) = A(s)B(s)$ Dirichletsche Reihe?
Man wende das insbesondere auf $A(s) = B(s) = \zeta(s)$ an.

44.) Sei eine Zufallsgröße X mit Werten in $\mathbb{N}_{\geq 1}$ gegeben, sowie $p_k = \mathbb{P}\{X = k\}$ und $P(z) = \sum_{k\geq 1} \frac{p_k}{k^z}$:

(a) Drücken Sie $\mathbb{E}(X)$, $\mathbb{V}(X)$, $\mathbb{E}(\log X)$ durch $P(z)$, $P'(z)$, etc. aus.

(b) Sei $Q(z) = \sum_{k\geq 1} \frac{q_k}{k^z}$ mit $q_k = \mathbb{P}\{Y = k\}$. X und Y seien unabhängig.
Was ist die erzeugende Funktion von $X \cdot Y$? Zeigen Sie:

$$\mathbb{E}(X \cdot Y) = \mathbb{E}(X) \cdot \mathbb{E}(Y),$$
$$\mathbb{V}(X \cdot Y) = (\mathbb{V}(X) + \mathbb{E}(X)^2)(\mathbb{V}(Y) + \mathbb{E}(Y)^2) - \mathbb{E}(X)^2\mathbb{E}(Y)^2.$$

Drücken Sie diese Größen durch P und Q aus!

45.) Es sei A ein Algorithmus gegeben, der zwei Polynome von Graden m und n (über $\mathbb{C}$) in $O((m+n)\log(m+n)$ Rechenoperationen (= Multiplikationen komplexer Zahlen) multipliziert. (Dabei werden die Polynome durch ihre Koeffizienten beschrieben).

Man entwickle daraus einen Algorithmus, der zwei natürliche Zahlen *schnell* multipliziert. (Die natürlichen Zahlen sind z.B. im Binärsystem gegeben und haben m bzw. n Ziffern.)

Übungsblatt 10 für Analyse von Algorithmen (12.12.2012)

46.) Für eine natürliche Zahl $N \geq 1$ sei $\zeta_N = e^{2\pi i/N}$ die (primitive) N-te Einheitswurzel und F_N die Matrix $F_N = (\zeta_N^{jk})_{0\leq j,k<N}$. Man zeige, dass die Matrix $F_N^{-1} = \frac{1}{N}(\zeta_N^{-jk})_{0\leq j,k<N}$ die zu F_N inverse Matrix ist.

47.) Man zeige: $H_n = \displaystyle\sum_{1\leq k\leq n} \binom{n}{k} \frac{(-1)^{k+1}}{k}$.

48.) Es sei $\mu(n)$, $n \geq 1$, die Möbiusfunktion:

$$\mu(n) = \begin{cases} 1 & \text{für } n = 1, \\ (-1)^r & \text{wenn } n \text{ das Produkt von } r \text{ verschiedener Primzahlen ist,} \\ 0 & \text{sonst.} \end{cases}$$

Man zeige die Beziehung $\displaystyle\sum_{d|n} \mu(d) = 0$ für $n > 1$ und beweise damit die Beziehung

$$b_n = \sum_{d|n} a_d \quad \Longleftrightarrow \quad a_n = \sum_{d|n} b_d\, \mu(n/d).$$

49.) Was kann man über die Dirichletsche Reihe $\sum_{n\geq 1} \mu(n) n^{-s}$ sagen?

50.) Es sei $A(x)$ eine erzeugende Funktion mit $A(0) = 0$ und $B(x)$ sei durch

$$B(x) = \sum_{k\geq 1} \frac{1}{k} A(x^k)$$

definiert. Man zeige

$$A(x) = \sum_{k\geq 1} \frac{\mu(k)}{k} B(x^k).$$

Übungsblatt 11 für Analyse von Algorithmen (19.12.2012)

51.) Sei K ein Körper. Für ein Polynom $f = \sum_k a_k x^k \in K[x]$ ist die formale Ableitung f' durch $f' = \sum_k (k+1) a_{k+1} x^k$ definiert (wobei k als Abkürzung für $k = 1 + 1 + \cdots + 1 = k \cdot 1$ steht). Man zeige die Ableitungsregeln $(fg)' = f'g + fg'$ und $(f^m)' = m f^{m-1} f'$.

52.) Es sei $f = f_1^{e_1} \cdots f_r^{e_r}$ die eindeutige Zerlegung eines normierten Polynoms über einem endlichen Körper in normierte irreduzible Polynome. Man formuliere einen Algorithmus, der bei Eingabe von f das Produkt $g = f_1 \cdots f_r$ bestimmt, ohne dass die Faktoren f_j bestimmt werden.
Hinweis: Man starte mit dem $\mathrm{ggT}(f, f')$.

53.) Man zeige: Über einem endlichen Körper mit q Elementen gilt für jedes $m \geq 1$

$$x^{q^m} - x = \prod f(x),$$

wobei das Produkt auf der rechten Seite über alle normierten irreduziblen Polynome $f(x)$ gebildet wird, deren Grad ein Teiler von m ist.
Hinweis: Man verwende die Eigenschaft, dass $x^{q^m} - x = \prod (x - \alpha)$ ist, wobei das Produkt über alle Elemente aus $\mathbb{F}_{q^m}$ gebildet wird, und fasse entsprechend zusammen.

54.) Sei q eine ungerade Primzahlpotenz und $S = \{b^2 : b \in \mathbb{F}_q^\times\}$ der Menge der Quadrate in $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$. Man zeige, dass S eine Untergruppe von $\mathbb{F}_q^\times$ der Ordnung $(q-1)/2$ ist und

$$S = \{a \in \mathbb{F}_q^\times : a^{(q-1)/2} = 1\}, \qquad \mathbb{F}_q^\times \setminus S = \{a \in \mathbb{F}_q^\times : a^{(q-1)/2} = -1\}.$$

55.) Für ein Element $a \in \mathbb{F}_{2^k}$ ist die Spur durch

$$\mathrm{Sp}(a) = \sum_{i=0}^{k-1} a^{2^i}$$

definiert. Man zeige, dass $\mathrm{Sp} : \mathbb{F}_{2^k} \to \mathbb{F}_2$ eine lineare Abbildung ist, bei der 0 und 1 gleichoft angenommen werden.

Übungsblatt 12 für Analyse von Algorithmen (9.1.2013)

56.) Es sei $f(x) \in \mathbb{F}_q$ ein Polynom mit $f' = 0$ und es bezeichne p die Charakteristik von $\mathbb{F}_q$. Man zeige, dass dann $f(x) = g(x)^p$ ist für ein Polynom $g(x) \in \mathbb{F}_q$.

57.) Man formuliere (z.B. mit Hilfe von Beispiel 55) einen Faktorisierungsalgorithmus für Polynome $f(x) \in \mathbb{F}_{2^k}[x]$.

58.) Es sei n eine naürliche Zahl mit Primfaktoren $p_1, \ldots, p_r$ Man zeige, dass ein normiertes Polynom $f(x) \in \mathbb{F}_q$ vom Grad n genau dann irreduzibel ist, wenn $f(x) | x^{q^n} - x$ gilt und wenn $\mathrm{ggT}(f(x), x^{q^{n/p_j}} - x) = 1$ für alle $j = 1, \ldots, r$ gilt.

59.) Ein Polynom $f(x) \in \mathbb{F}_q$ heißt *primitiv*, wenn $f(x)$ irreduzibel ist und eine Nullstelle von $f(x)$ ein erzeugendes Element der multiplikativen Gruppe von $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f(x))$ ist. Wie kann man (algorithmisch) feststellen, ob ein gegebenes Polynom primitiv ist?
Hinweis: Man beachte, dass die Restklasse $\alpha = x \bmod f(x)$ ein erzeugendes Element von $\mathbb{F}_q[x]/(f(x))$ sein muss.

60.) Es sei $C_m = \{g, g^2, \ldots, g^m = 1\}$ eine zyklische Gruppe der Ordnung m mit erzeugendem Element g. Man zeige:

$$\#\{x \in C_m : x^k = 1\} = \mathrm{ggT}(k, m).$$

Übungsblatt 13 für Analyse von Algorithmen (16.1.2013)

61.) Man zeige, dass es für jede ungerade natürliche Zahl n, die keine Primzahl ist, ganze Zahlen a, b mit $n = a^2 - b^2$ gibt.

62.) Es sei g eine Primitivwurzel modulo einer ungeraden Primzahl p (d.h. die Restklasse $\overline{g}$ ist ein erzeugendes Element der Gruppe $\mathbb{Z}_p^*$). Man zeige, dass dann g oder $g + p$ ein erzeugendes Element der multiplikative Gruppe $\mathbb{Z}_{p^2}^*$ bildet.

63.) Man untersuche den Aufwand eines Durchlaufs des Miller-Rabin-Tests.

64.) Die Folgen U_n, V_n und L_n sind induktiv definiert:

$$\begin{aligned} U_0 &= 0,\ U_1 = 0,\ U_{n+1} = 4U_n - U_{n-1}, \\ V_0 &= 2,\ V_1 = 4,\ V_{n+1} = 4V_n - V_{n-1}, \\ L_0 &= 4,\ L_{n+1} = L_n^2 - 2. \end{aligned}$$

Man zeige die Identitäten

$$\begin{aligned} V_n &= U_{n+1} - U_{n-1}, \\ U_n &= \left((2+\sqrt{3})^n - (2-\sqrt{3})^n\right)/\sqrt{12}, \\ V_n &= (2+\sqrt{3})^n + (2-\sqrt{3})^n, \\ U_{n+m} &= U_m U_{n+1} - U_{m-1} U_n \\ L_n &= V_{2^n}. \end{aligned}$$

65.) Man zeige weiters $\mathrm{ggT}(U_n, U_{n+1}) = 1$ und $\mathrm{ggT}(U_n, V_n) \leq 2$.