Diskrete und geometrische Algorithmen
Übung 11

8. Jänner 2024

1. Alice hat den öffentlichen Schlüssel $n = 89081, e = 43$. Bob schickt ihr eine mittels RSA-Verfahren verschlüsselte Nachricht mit dem Wert $c = 42709$.
   Ein Angreifer möchte diese Nachricht entschlüsseln. Bestimmen Sie dazu d via $ed = 1 + (p-1)(q-1)y$ mithilfe des erweiterten euklidschen Algorithmus (dazu ist zunächst die Primfaktorzerlegung $n = pq$ vonnöten, um $(p-1)(q-1)$ bestimmen zu können). Berechnen Sie anschließend die Nachricht $m = c^d (\text{mod } n)$.

2. Das *Sieb des Erathostenes* ist ein Algorithmus, der alle Primzahlen kleinergleich einer gegebenen natürlichen Zahl n findet. Er arbeitet wie folgt:
   1.) Erstelle eine Liste aller ganzen Zahlen von 2 bis n.
   2.) Zu Beginn, sei $p = 2$ (die kleinste Primzahl).
   3.) Markiere die Vielfachen von p in der Liste, indem man von $2p$ bis n in Schritten der Länge p zählt.
   4.) Finde die erste Zahl in der Liste, die größer als p und noch nicht markiert ist. Wenn es keine solche Zahl gibt, gehe zum nächsten Schritt. Andernfalls sei p nun diese Zahl (die nächstgrößere Primzahl) und wiederhole Schritt 3.
   5.) Gebe alle nicht markierten Zahlen auf der Liste aus. Dies sind die Primzahlen kleiner gleich n.

   (a) Führen Sie das Sieb des Erathostenes anhand der Zahlen von 1 bis 100 durch.
   (b) Beschreiben Sie das Sieb des Erathostenes als Pseudocode.

3. Beweisen Sie folgende Eigenschaft für komplexe Einheitswurzeln: Sei ω_n eine primitive n-te Einheitswurzel. Dann ist ω_n^k eine primitive $\frac{n}{\text{ggT}(n,k)}$-te Einheitswurzel.

4. Erklären Sie die Funktionsweise des FFT-Algorithmus anhand der Berechnung des Produkts der
   Polynome $A(x) = 4 - 4x$ und $B(x) = 6 + 2x$.

5. Gegeben sei der n-periodische diskrete Rechtecksimpuls $\mathbf{a} = (a_k)_k$ mit $a_0 = a_{n-1} = 1$ und $a_j = 0$ für $j = 1, 2, \ldots, n-2$. Berechnen Sie $\mathrm{DFT}_n(\mathbf{a})$.

6. Wir betrachten nun allgemeiner "Wechsel-Geld-Problem" (WGK). In einer Währung existieren (unlimitiert viele) Münzen im Wert von $1 = d_1 < d_2 < \cdots < d_k$ Cent. Ziel des WGK ist es, mit möglichst wenigen Münzen einen gegebenen Betrag von n Cent zu wechseln.

   (a) Bestätigen Sie, dass das WGK die optimale Teilstruktur-Eigenschaft erfüllt, d.h., zeigen Sie, dass eine optimale Lösung für n Cent, d.h., $n = \sum_i c_i d_i$ und $\sum_i c_i$ ist minimal, auch eine optimale Lösung für b bzw. $n - b$ Cent darstellt, wenn b ein Anteil von n ist, welcher durch die in der Darstellung von n verwendeten Münzen zustande kommt, d.h., $b = \sum_i c'_i d_i$ und $c'_i \leq c_i$.

   (b) Sei $A(n)$ die Anzahl der Münzen, die zum Wechseln des Betrags n mindestens notwendig sind. Überlegen Sie sich eine Rekursion für $A(n)$.

   (c) Erklären Sie die Funktionsweise des folgenden Algorithmus $\textsc{Wechsel}(d, k, n)$, welcher für den Wert n und für ein gegebenes Münzen-Array $d = (d_1, \ldots, d_k)$ die optimale Wechsellösung liefert am Beispiel $(d_1, d_2, d_3) = (1, 2, 5)$ und $n = 8$.

```
WECHSEL(d, k, n)
seien C[0..n] und S[0..n] neue Felder
C[0] := 0
for j = 1 to n do
    C[j] := ∞
    for i = 1 to k do
        if d_i ≤ j and 1 + C[j − d_i] < C[j] then
            C[j] := 1 + C[j − d_i]
            S[j] := d_i
        end if
    end for
end for
return C und S
```

   (d) Wie groß ist asymptotisch die Komplexität von $\textsc{Wechsel}(d, k, n)$?