Junior-Prof. Dr. Robert Elsässer, Marco Muñiz, Phillip Heidegger WS 2009/2010

Algorithms Theory, Assignment 2

http://lak.informatik.uni-freiburg.de/lak_teaching/ws09_10/algo0910.php

Submission: 19. Nov. 2009, 4 p.m.

- The solutions can be submitted in English or German
- You are required to submit your own solution.
- You are allowed to discuss with each other. Nevertheless, you are required to write down the answers in your own words.

Exercise 2.1 - Fast Fourier Transform [Points: 6]

Compute the product of the two polynomials

$$p(x) = 3x + 1 \quad \text{and} \quad q(x) = 7x + 4$$

using FFT and interpolation.

Exercise 2.2 - Fast Fourier Transform [Points: 6+Bonus 2]

Let A and B be two sets of integers in the range of $[0, m-1]$ where m is a power of two. Show that the following can be computed in $\mathcal{O}(m \log m)$ time with a single DFT:

1. All elements contained in the set $A + B = \{c \mid a \in A, b \in B, c = a + b\}$
2. For each $c \in [0, \ldots, 2m-2]$, the number $k_c = |\{(a, b) \in A \times B \mid a + b = c\}|$.
3. For each $x \in [1, \ldots, 2m-2]$, the number

$$d_x = |\{(a, b) \mid (a, b) \in A \times B, a + b | x\}| \quad .$$

For two natural numbers $a, b \in \mathbb{N}$ we Define $a|b$ as "b is divisible by a" or "a divides b".

$$a|b \quad \text{iff} \quad \exists c \in \mathbb{N} : c \cdot a = b$$

Hint: Find some polynomials p_A, p_B of degree less than m that represent the sets A and B.

Exercise 2.3 - Randomized Quicksort [Points: 4]

1. Consider a variant of the randomized Quicksort algorithm, in which only l or r (leftmost,rightmost element) can be taken with probability p_l and p_r as pivot elements. Further, consider the set $n = \{n_1, n_2, \ldots, n_m\}$ where $n_i < n_j$ for $i < j$, $0 < i$ and $j \leq m$. Give 3 permutations π of n and 3 different assignments for p_l and p_r such that $T(n) = \Theta(n^2)$.
2. The expected runtime of randomized Quicksort is for $n > 1$

$$T(n) = \frac{2}{n} \sum_{k=1}^{n-1} T(k) + \Theta(n)$$

while $T(1) = c$ for some $c \in \mathbb{N}$.

Prove that $T(n) \in \mathcal{O}(n \log n)$.

Exercise 2.4 - RSA

[Points: 4]

For an RSA encryption choose $p = 19$, $q = 29$ and let $e = 5$.

1. Compute the number d and give the output of the executed extended−Euclid algorithm. In addition, compute the secret and public keys.
2. By using the public key, cypher the decimal message $M = 22$.