Matthias Westermann, Marco Muñiz WS 2010/2011

Algorithms Theory, Assignment 2

Submission: hand in by 17. Nov. 2010

Exercise 2.1 - Fast Fourier Transform [Points: 5]

Compute the product of the two polynomials

$$p(x) = 7x + 3 \text{ and } q(x) = 5x + 11$$

using FFT and interpolation.

Exercise 2.2 - Fast Fourier Transform [Points: 5]

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 $A + B = \{c \mid a \in A, b \in B, c = a + b\}$

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

Exercise 2.3 - Primality test [Points: 5]

Consider the number $n = 1105$. Use the randomized primality test algorithm with $a = 7$ to determine if n is probably prime or not prime. Each recursive call and each intermediate value of result should be provided.

```
bool isProbPrime;

bool primeTest(int n)
{
  isProbPrime = true;
  a = 7;
  result = power(a,n-1,n);
  if (result !=1 || !isProbPrime)
    return false;
  else
    return true;
}
```

```
int power(int a, int p, int n) {
  if (p==0)
    return 1;
  x = power(a,p/2,n);
  result = (x*x)%n;
  if (result==1 && x!=1 && x!=n-1) {
    isProbPrime = false;
  }
  if (p%2==1)
    result = (a*result)%n;
  return result;
}
```

Exercise 2.4 - RSA [Points: 5]

For an RSA encryption choose $p = 13$, $q = 19$ and let $e = 7$.

1. Compute the number d and give the output of the executed extended-Euclid algorithm.
2. By using the public key, encrypt the decimal message $M = 16$.
3. Decrypt the message $M' = 151$.