Self-study session 4, Discrete mathematics

First year mathematics for the technology and science programmes
Aalborg University

This self-study session consists of two parts: fast multiplication-algorithm and RSA cryptography.

Fast multiplication-algorithm

> *" In 1960, Kolmogorov organized a seminar on mathematical problems in cybernetics at the Moscow State University, where he stated the $\Omega(n^2)$ conjecture and other problems in the complexity of computation. Within a week, Karatsuba, then a 23-year-old student, found an algorithm (later it was called "divide and conquer") that multiplies two n-digit numbers in $\Theta(n^{\log_2(3)})$ elementary steps, thus disproving the conjecture. Kolmogorov was very agitated about the discovery; he communicated it at the next meeting of the seminar, which was then terminated. Kolmogorov published the method in 1962, in the Proceedings of the USSR Academy of Sciences. The article had been written by Kolmogorov, possibly in collaboration with Yuri Ofman, but listed "A. Karatsuba and Yu. Ofman" as the authors. Karatsuba only became aware of the paper when he received the reprints from the publisher."*
>
> *(Wikipedia)*

In this section we will work on a divide-and-conquer algorithm. It is essential that you understand the the recursive nature of this type of algorithm.

Karatsuba's algorithm

Read Example 4 (Fast Multiplication of Integers) in section 8.3 in Rosen's bog very thoroughly. The algorithm described in this example is known as "Karatsuba's algorithm".
Also read Example 10 in section 8.3.

Go to Wikipedia and see what it says about Karatsuba's algorithm. For very large numbers Karatsuba's algorithm is faster that the usual multiplication algorithm. Find in the Wikipedia page information about, how large numbers should be to make Karatsuba's algoritm faster than traditional multiplication. Describe these numbers in base 10, so that you can relate to their size.

Below Karatsuba's algorithm is applied to computation of $7 \cdot 13$. Follow the computations thoroughly and make sure you understand what is going on.

First we find the binary expansions: $7 = (0111)_2$ and $13 = (1101)_2$. The binary representations

are of size $4 = 2n$, where $n = 2$. The computations are as follows:

$$
\begin{aligned}
&(0111)_2(1101)_2 \\
=&(2^4+2^2)\Big\{(01)_2(11)_2\Big\} + 2^2\Big\{\big((01)_2-(11)_2\big)\big((01)_2-(11)_2\big)\Big\} + (2^2+1)\Big\{(11)_2(01)_2\Big\} \\
=&(2^4+2^2)\Big\{(01)_2(11)_2\Big\} + 2^2\Big\{(10)_2(10)_2\Big\} + (2^2+1)\Big\{(11)_2(01)_2\Big\} \\
=&(2^4+2^2)\Big\{(2^2+2)(0)_2(1)_2 + 2\big((0)_2-(1)_2\big)\big((1)_2-(1)_2\big) + (2+1)(1)_2(1)_2\Big\} \\
&+2^2\Big\{(2^2+2)(1)_2(1)_2 + 2\big((1)_2-(0)_2\big)\big((0)_2-(1)_2\big) + (2+1)\big((0)_2(0)_2\big)\Big\} \\
&+(2^2+1)\Big\{(2^2+2)(1)_2(0)_2 + 2\big((1)_2-(1)_2\big)\big((1)_2-(0)_2\big) + (2+1)(1)_2(1)_2\Big\} \\
=&(2^4+2^2)\Big\{(2^2+2)(0)_2 - 2(1)_2(0)_2 + (2+1)(1)_2\Big\} \\
&+2^2\Big\{(2^2+2)(1)_2 - 2(1)_2(1)_2 + (2+1)(0)_2\Big\} \\
&+(2^2+1)\Big\{(2^2+2)\big((0)_2 + 2(0)_2(1)_2 + (2+1)(1)_2\Big\} \\
=&(2^4+2^2)\Big\{-2(0)_2 + (10)_2 + (1)_2\Big\} \\
&+(2^2\Big\{(100)_2 + (10)_2 - (10)_2\Big\} \\
&+(2^2+1)\Big\{2(0)_2 + (10)_2 + (1)_2\Big\} \\
=&(2^4+2^2)(11)_2 + 2^2(100)_2 + (2^2+1)(11)_2 \\
=&(110000)_2 + (1100)_2 + (10000)_2 + (1100)_2 + (11)_2 \\
=&(1011011)_2
\end{aligned}
$$

We get that $(1011011)_2 = 64 + 16 + 8 + 2 + 1 = 91$ as expected.

Note that in the above computation we postpone e.g. multiplications by 2^4 until the end. This is because this multiplication just corresponds to adding four 0's at the end of the number. Similarly for other powers of 2. Also note that some negative numbers may appear in the calculation.

Now solve exercise 14 from the exam 17. januar 2011 (EVU), see `http://first.math.aau.dk/dan/2017f/dmat/#tab_oldexams` or see an English translation in Section 3 below. This exercise requires more work than usuall for an 8-point exercise. The text refers to an earlier edition of Rosen's book, but it is still Example 4.

Solve exercise 3 in section 8.3

RSA-cryptography

Read the pages 295–298 in Rosen's book.

Solve these exercises from Rosen, section 4.6: **14**, **15**, **13**.

Solve exercise 3 from exam 17. januar 2011 (EVU).

Opgave

- Use the Maple command "isprime" to find three-digit prime numbers p and q of you own choice (keep trying until isprime(...)=true).
- Define $m = (p-1)(q-1)$ and $n = pq$.
- Find (by trial and error) a number e (do NOT choose $e = 1$) so that $\gcd(e, m) = 1$. Use the extended Euclidian algorithm to find an integer d, so that $de \equiv 1 \pmod{m}$. This can also be done using the Maple command "igcdex(e,m,u,v)".
- Then the public key is "(n, e)" and the private key is "d".
- Use the public key to encode a positive number M less than n. Call this number C. Then decode C using the private key (and n which known to everybody).

Exam 17. januar 2011

Here it an English translation of two exercises from this old exam.

Opgave 3: (8 %) Use the chinese remainder algorithm to find all integers x satisfying that

$$x \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{4}$$

$$x \equiv 3 \pmod{5}$$

Opgave 14: (8 %)

1. Determine the binary expansions of 13 and 15.
2. Compute the product of the two numbers from question 1, using the fast multiplication algoritm (Example 4 in Section 8.3 in Rosen).