Selvstudium 4, Diskret matematik

Matematik på første studieår for de tekniske og naturvidenskabelige uddannelser
Aalborg Universitet

Dette selvstudium består af to dele: hurtig multiplikations-algoritme og RSA kryptering.

Hurtig multiplikations-algoritme

> *" 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."*
>
> *(Den engelske Wikipedia)*

I dette afsnit skal vi arbejde med en del-og-hersk-algoritme. Det er essentielt, at man forstår den rekursive natur af disse.

Karatsubas algoritme

Læs eksempel 4 (Fast Multiplication of Integers) i afsnit 8.3 i Rosens bog meget grundigt. Den beskrevne algoritme er kendt under navnet "Karatsubas algoritme".
Læs desuden eksempel 10 i afsnit 8.3.

Gå til den engelske wikipedia og find siden om Karatsubas algoritme (brug altid den engelske wikipedia, når du søger teknisk information). For meget store problemstørrelser er Karatsubas algoritme hurtigere end traditionel multiplikation. Find i teksten information om, hvor store tallene skal være for at Karatsubas algoritme er bedst. Beskriv disse tal i base 10, for at forholde dig til deres egentlige størrelse.

Nedenfor anvendes Karatsubas algoritme på udregningen af $7 \cdot 13$. Følg udregningerne nøje, og vær sikker på, at du forstår, hvad der foregår.

Først findes de binære ekspansioner: $7 = (0111)_2$ og $13 = (1101)_2$. De binære repræsentationer

er altså af størrelse $4 = 2n$, hvor $n = 2$. Udregningerne er som følger:

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

Vi har $(1011011)_2 = 64 + 16 + 8 + 2 + 1 = 91$ som forventet.

Bemærk i ovenstående udregninger, at vi eksempelvis gemmer multiplikationerne med 2^4 til sidst. Det er fordi, det bare svarer til at tilføje fire 0'er i enden. Tilsvarende med andre potenser af 2. Bemærk også, at vi kan komme ud for negative tal undervejs.

Regn nu opgave 14 fra eksamen 17. januar 2011 (EVU), se `http://first.math.aau.dk/dan/2018f/dmat/#tab_oldexams`. De 8 point, som opgaven er anført til er i underkanten. Sidetallet i opgaven henviser til en tidligere udgave af bogen.

Regn dernæst opgave 3 i afsnit 8.3

RSA-kryptering

Herefter arbejder vi med RSA-kryptografi. Læs og forstå side 295 til side 298 i Rosens bog.

Lav disse opgaver fra Rosen, afsnit 4.6: **14**, **15**, **13**.

Regn nu opgave 3 fra eksamen 17. januar 2011 (EVU).

Opgave

- Find vha. Maplekommandoen "isprime" to trecifrede primtal p og q efter eget valg (du skal prove dig frem indtil isprime(...)=true).
- Definér $m = (p-1)(q-1)$ og $n = pq$.
- Find (ved at prove dig frem) et tal e (vælg IKKE $e = 1$) så $\gcd(e, m) = 1$. Find vha. Euklids udvidede algoritme et heltal d, så $de \equiv 1 \pmod{m}$. Dette kan også beregnes med Maplekommandoen "igcdex(e,m,u,v)".
- Offentlig nogle er nu "(n, e)". Hemmelig nogle er "d".
- Indkod vha. den offentlige nogle et positivt tal M mindre end n. Kald det C. Dekod det derefter vha. den hemmelige nogle (samt n, som jo er kendt af alle).