Heltal, modulus og Extended Euclidean Algorithm

af Jacob Allerelli

October 12, 2005

Først lidt om de tal vi arbejder med:

$\mathbb{N} = \{1, 2, \dots\}$: mængden af positive heltal.
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$: mængden af alle heltal.
$\mathbb{Q}$: mængden af rationelle tal, hvor $q \in \mathbb{Q}$ kan skrives som $q = \frac{a}{b}$, hvor $a \in \mathbb{Z}$ og $b \in \mathbb{N}$.
$\mathbb{R}$: mængden af rationelle og irrationelle tal (f.eks. $\pi, \sqrt{2}, \dots$).
For ovenstående talmængder gælder at

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Vi lægger blødt ud med en definition af hvad det vil sige "at gå op i".

Definition ("at gå op i")
Lad $a, q \in \mathbb{Z}$ med $q \neq 0$. Vi siger at q går op i a, hvis der findes et $d \in \mathbb{Z}$ sådan at $a = dq$ og vi skriver det $q|a$. Desuden kalder vi d og g for a's faktorer.

Definition (primtal)
Et $p \in \mathbb{N}$ hvor $p > 1$ kalds et primtal, hvis de eneste positive faktorer for p er 1 og p.

Bemærk: hvis $q \nmid a$ (q går ikke op i a) må der findes et $r \in \mathbb{N}$ sådan at $a = dq + r$ med $0 \leq r < d$. Dette leder os frem til.

Sætning (The Division Algorithm)
Lad $a \in \mathbb{Z}$ og $d \in \mathbb{N}$, så findes der entydigt bestemte tal $q, r \in \mathbb{Z}$ med $0 \leq r < d$, sådan at

$$a = dq + r,$$

hvor d kaldes divisoren, a dividenten, q kvotienten og r resten.

Notation (kvotient og rest)
Man bruger følgende notation for kvotienten og resten:

$$q = a \text{ div } d, \quad r = a \bmod d,$$

hvor mod står for modulo.

Definition (kongruens)
Lad $a, b, c, d \in \mathbb{Z}$ og $m \in \mathbb{N}$, så siger vi at a er kongruent med b, hvis $m|(a-b)$ og vi skriver det $a \equiv b \pmod{m}$ for at indikere at a er kongruent med b modulo m.

Man kan vise følgende "regneregler" for modulo:

Regneregler for modulo
Lad $a, b \in \mathbb{Z}$ og $m \in \mathbb{N}$. Da gælder følgende

$$a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$$

$$a \equiv b \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z} : a = b + km$$

$$a \equiv b \pmod{m} \text{ og } c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$$

$$a \equiv b \pmod{m} \text{ og } c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$$

Vi haster lystigt videre til definitionen på største fælles divisor.

Definition (største fælles divisor el. greatest common divisor)
Lad $a, b \in \mathbb{Z}$ med $a \neq 0$ eller $b \neq 0$. Det største heltal $d \in \mathbb{Z}$ sådan at $d|a$ og $d|b$ kaldes den største fælles divisor for a og b og betegnes $\gcd(a, b)$.
NB: hvis $\gcd(a, b) = 1$ siger man at a og b er indbyrdes primiske.

Sætning
Lad $a, b \in \mathbb{N}$, så findes der $s, t \in \mathbb{Z}$ sådan at $\gcd(a, b) = as + tb$.

Bemærk: Den "udvidede Euklidiske algoritme" (Extended Euclidean Algorithm) finder både $\gcd(a, b)$ og s og t.

Definition (multiplikativ invers)
Lad $a \in \mathbb{Z}$ og $m \in \mathbb{N}$. Hvis der eksisterer et $b \in \mathbb{Z}$ så $ab \equiv 1 \pmod{m}$, da siger man at a har en multiplikativ invers og denne er b. Man kalder ofte den multiplikative inverse a^{-1}.

Sætning
Lad $a, m \in \mathbb{N}$ være indbyrdes primiske og $m > 1$. Så eksisterer der en entydig multiplikativ invers a^{-1} til $a \bmod m$

References

[1] Kenneth H. Rosen.
Discrete Mathematics and Its Applications, 5th ed..
Mc Graw Hill, 2001.